Matematicamente.it

Germano Pettarin

IT Security
modulo 5 della nuova ecdl

E-book per la preparazione della Nuova ECDL



 ISBN 9788896354742

Germano Pettarin
IT Security, modulo 5 della Nuova ECDL
E-book per la preparazione della Nuova ECDL
Copertina: Ginger Lab - www.gingerlab.it
Immagine di copertina: Slutspurten by Patrick Strandberg

www.matematicamente.it - info@matematicamente.it
Novembre 2014
ISBN 9788896354742

SOMMARIO

Introduzione:

Modulo IT Security

Scopi del modulo

Il presente modulo definisce i concetti e le competenze fondamentali per comprendere l'uso sicuro dell'Information e Communication Tecnology nelle attività quotidiane e per utilizzare tecniche e applicazioni rilevanti che consentono di gestire una connessione di rete sicura, usare Internet in modo sicuro e senza rischi e gestire in modo adeguato dati e informazioni.
Gli argomenti sviluppati in questo modulo sono:

- Comprendere i concetti fondamentali relativi all'importanza di rendere sicure informazioni e dati, di assicurare protezione fisica e privacy, e di difendersi dal furto di identità.
- Proteggere un computer, un dispositivo o una rete da malware e da accessi non autorizzati.
- Comprendere i tipi di reti, i tipi di connessioni e le problematiche specifiche alle reti, firewall inclusi.
- Navigare nel World Wide Web e comunicare in modo sicuro su Internet.
- Comprendere i problemi di sicurezza associati alle comunicazioni, inclusa la posta elettronica e la messaggistica istantanea.
- Effettuare copie di sicurezza e ripristinare i dati in modo corretto e sicuro, ed eliminare dati e dispositivi in modo sicuro.

Con questo modulo sono certificate le capacità di individuare e comprendere i concetti principali alla base di un uso sicuro della Tecnologia dell'Informazione e Comunicazione (ICT) e le competenze per proteggere i propri dati e quelli dell'organizzazione per la quale si lavora.

Capitolo 1

Minacce ai dati

Salvaguardare le informazioni

Distinguere tra dati e informazioni.

- I **dati** sono informazioni non ancora sottoposte a elaborazione. I dati possono essere una collezione di numeri, testi o immagini non elaborate. Dall'elaborazione dei dati si ottengono le:
- **informazioni** sono il risultato dell'utilizzo dei dati e della loro eventuale modifica in modo da renderli significativi per la persona che li riceve.

Comprendere il termine crimine informatico.

Il **crimine informatico** è un'attività illegale che avviene utilizzando dei mezzi informatici come la rete Internet o, in generale, un computer. Esempi di crimine informatico includono le frodi informatiche, il furto di identità e l'intrusione nei sistemi informatici.
Le frodi informatiche possono riguardare la riproduzione e/o l'utilizzo di programmi informatici senza la specifica autorizzazione. Infatti, i programmi informatici sono ritenuti opere dell'ingegno e quindi sono tutelati dalla legge sul diritto d'autore. Le frodi informatiche possono riguardare anche la vendita on line di prodotti inesistenti o contraffatti.
I programmi informatici quindi non possono essere usati e duplicati senza autorizzazione.
In generale non è consentito:

1. fare delle copie non autorizzate di un software o di parte di esso;
2. andare a vedere e copiare il modo con cui è stato realizzato;
3. installarlo su diversi computer senza autorizzazione o cederlo ad altri.

Infatti, quando si acquista un programma non si diventa proprietari del software senza alcun vincolo: non si può fare un libero uso del programma, ma si acquisisce soltanto la **licenza d'uso**, detta **EULA**.
EULA o End User License Agreement (accordo di licenza con l'utente finale) è il contratto tra il fornitore del software e l'utente finale. Tale contratto assegna la licenza d'uso del programma all'utente nei termini stabiliti dal contratto stesso. EULA solitamente permette soltanto:

1. di utilizzare il software su un solo computer, salvo diverse indicazioni (contratti multi licenza);
2. la possibilità di fare una ulteriore copia, la copia di sicurezza, del supporto con cui il software è distribuito. È quindi possibile duplicare il cd del programma ma solo per creare la copia di sicurezza.

Quindi è un reato:

1. installare lo stesso programma su più computer, se non è espressamente consentito nella licenza;

2. avere una copia illegale di un programma;
3. scambiare o scaricare tramite internet musica, testi, film soggetti alla tutela del copyright;
4. modificare del software e personalizzarlo per rivenderlo come proprio.

Per riconoscere software regolarmente licenziato si deve verificare il codice del prodotto, il numero di registrazione del prodotto (Product Key) o visualizzare la licenza del software.
Un codice di licenza è una serie di numeri e lettere utilizzata per installare e registrare le versioni del software. Questi codici si possono trovare nella scatola del prodotto, sul supporto con cui è stato distribuito il software, nel certificato di autenticità generalmente riportato sul computer.



Le licenze software quindi sono documenti legali allegati ai programmi. Senza un tale documento, un programma non può essere distribuito né modificato senza l'esplicito consenso degli autori.

Differenza tra Hacking, Kracking e Hacking etico

L’attività di **Hacking** (dall’inglese to hack, intaccare) è svolta da programmatori (hacker) che si collegano e accedono a risorse di rete senza averne l’autorizzazione, solo per gusto di sfidare il computer e i sistemi di protezione. Solitamente un hacker non vuole causare un danno ma usare le risorse del sistema attaccato oppure semplicemente dimostrare di essere riuscito ad accedervi.
Quando la violazione di un sistema da parte di un hacker comporta un vantaggio personale o un uso delle risorse per proprio lucro, si parla di **Kracking**: ad esempio, rubare o alterare dei dati, danneggiare il sistema, ecc. Per kracker si intende anche un programmatore che si dedica alla pirateria informatica, rimuovendo le protezioni dai programmi e distribuendone copie illegalmente a scopo di lucro. Alcuni esempi di attività di kracking sono il **Cracking di password**, cioè il recupero di password, in modo manuale o con appositi programmi, da dati memorizzati o inviati ad un sistema informatico e il **Cracking di software**, cioè la disattivazione o l’eliminazione di alcune funzioni del software come la protezione contro la copia, i numeri di serie, le chiavi hardware, i controlli di data, ecc.

A volte le competenze e le abilità di un hacker possono essere utilizzate “a fin di bene” per testare il grado di sicurezza di un sistema informatico. In questo caso si parla di **hacking etico**: l'utilizzo delle tecniche di hacking per monitorare la sicurezza dei sistemi e delle reti informatiche al fine di evitare l'abuso da parte di malintenzionati. In pratica è permesso l’attacco al sistema di sicurezza di un computer da parte dei proprietari per rilevarne le vulnerabilità.
Un famoso hacker che è diventato un hacker etico è Kevin David Mitnick, nome in codice “Condor”. Negli anni ’90 si è introdotto illegalmente nei sistemi informatici di varie società americane, sia sfruttando i *bug* (letteralmente “bachi”: errori nella scrittura di un software) dei loro sistemi informatici sia utilizzando la tecnica dell’*ingegneria sociale*, cioè acquisendo informazioni riservate direttamente dalle persone coinvolte nei sistemi informatici dell’azienda guadagnando la loro fiducia con l’inganno.
Ha eseguito tra le più ardite intrusioni nei computer del governo degli Stati Uniti. Dopo essere stato catturato e aver scontato diversi anni di carcere ha iniziato ad occuparsi di sicurezza informatica e attualmente è amministratore delegato di una azienda di consulenza e sicurezza.

Riconoscere le minacce ai dati provocate da forza maggiore.

Per **Forza maggiore** si intende una forza superiore o un evento imprevisto che può minacciare la conservazione dei dati. Queste forze o eventi possono essere naturali o generate dall’uomo. Ad esempio incendi, inondazioni, terremoti, guerre, furti, atti vandalici, ecc. In vista di questi frangenti è opportuno adottare delle misure di sicurezza per ridurre al minimo il danno che ne può derivare.
Una buona norma da seguire è assicurarsi che per tutti i dati importanti esista una copia di *riserva*, una copia di *backup*. È consigliabile conservare anche una copia dei software che sono installati nel computer.
Come vedremo nei capitoli successivi fare il backup significa copiare i dati su di un supporto esterno come un hard disk rimovibile, un CD/DVD riscrivibile, una chiave USB, ecc. Esistono dei programmi che creano automaticamente, mentre si lavora, copie di riserva dei dati.
È fondamentale che la copia di backup non sia conservata nelle vicinanze del computer che contiene i dati originari, per evitare che una delle calamità descritte in precedenza porti alla perdita di entrambe le copie.
Esistono servizi in Internet che offrono la possibilità di effettuare dei backup su dispositivi messi in rete: si chiamano **memorie online**, o dischi virtuali. Uno memoria online è come in un magazzino, un hard disk virtuale, uno spazio di memoria in un sito internet che si apre solo se si possiede la password di accesso. È un sistema avanzato di backup per avere una copia dei propri dati immediatamente accessibile anche in caso di emergenza. Basta collegarsi alla rete, dovunque ci si trovi senza avere il proprio computer. Un esempio di questo servizio è Dropbox.
Inoltre può essere utile come spazio per scambio di file tra utenti (chiaramente tutti in possesso della password).

Minacce ai dati provocate da impiegati, fornitori di servizi e persone esterne

I dati privati e personali di un utente, di una azienda, di una scuola, di un ospedale, ecc. sono un bene da proteggere, sia per evitare il furto di know how aziendale sia perché c'è una legislazione sulla privacy dei dati riservati molto rigorosa.
Abbiamo visto a quali rischi possono essere soggette queste informazioni. Ma la sicurezza dei dati di una organizzazione può essere minacciata anche dagli utilizzatori di questi dati o da persone esterne che accedono casualmente ad essi.
Ad esempio, gli stessi **impiegati**, con le loro azioni, possono compromettere le informazioni importanti dell'azienda dove lavorano: in modo accidentale, cancellando o modificando questi dati o per scopi fraudolenti, ad esempio rubando e vendendo alla concorrenza le specifiche dei prodotti.
Anche i **fornitori di servizi**, ad esempio gli addetti alla manutenzione dell'hardware e del software, potrebbero accedere casualmente a informazioni e dati e provocare, in modo volontario o meno, dei danni.
In ultima analisi, se delle **persone esterne** possono accedere al sistema informatico senza alcun controllo, ad esempio nel caso di una rete Wi-Fi senza chiavi di protezione, i dati sono a rischio di furto o danneggiamento.
Per evitare le problematiche esposte è importante che l'incaricato alla conservazione dei dati riservati o elenchi di aziende, di persone o banche dati deve salvaguardarli dall'intrusione di altri soggetti e non divulgarli se non con esplicita autorizzazione. Un modo è impostare una corretta gestione degli accessi attraverso autorizzazioni e password.

Domande

1. Il servizio offerto da DropBox rientra nell'ambito del Cloud Storage
    a. Vero
    b. Dipende dai file
    c. Dipende dal sistema operativo utilizzato
    d. Falso
2. Quale può essere una minaccia ai dati riservati in un ufficio?
    a. Un impiegato interno
    b. Un consulente
    c. Un fornitore esterno
    d. Tutte le risposte sono corrette

Per le risposte corrette vai all'ultima pagina del libro.

Capitolo 2

Valore delle informazioni

Importanza delle informazioni

Motivi per proteggere le informazioni personali

I motivi per cui è importante proteggere i dati riguardanti le proprie informazioni personali spesso sono abbastanza evidenti. Si pensi alle conseguenze di un accesso al proprio conto corrente bancario da parte di una persona che non sia il proprietario.
Un fenomeno frequente, nel campo della violazione dei dati personali, è il **furto d'identità**. Il furto d'identità consiste nell'ottenere indebitamente le informazioni personali di un soggetto al fine di sostituirsi in tutto o in parte al soggetto stesso e compiere azioni illecite in suo nome o ottenere credito tramite false credenziali.
Le informazioni personali carpite possono essere: nome, cognome, indirizzo, codice fiscale, numero di telefono/cellulare, luogo e data di nascita, numero della carta di credito, estremi del conto corrente, nome dei figli, ecc.
L'attività di carpire informazioni ingannando un utente ed indurlo a rivelare dati sensibili e personali come le credenziali di accesso al proprio conto online è detta **ingegneria sociale**.
L'ingegneria sociale si riferisce alla manipolazione delle persone, che vengono portate ad eseguire delle azioni o a divulgare informazioni riservate, invece di utilizzare tecniche di hacking per ottenere le stesse informazioni.
Attraverso operazioni di ingegneria sociale è possibile:

- Raccogliere informazioni riservate o di valore.
- **Realizzare frodi**, utilizzando le informazioni raccolte per commettere atti fraudolenti.
- **Accedere a sistemi informatici** in modo non autorizzato e, di conseguenza, consentendo potenzialmente l'accesso ad altre informazioni riservate.

Il fenomeno dell'ingegneria sociale è cresciuto proporzionalmente al diffondersi della rete internet. Infatti, nell'enorme mare di dati presente in internet è semplice reperire informazioni su una persona o un'azienda.
A tutti coloro che usano internet viene chiesto regolarmente di fornire dati personali per poter accedere a determinati siti o per poter acquistare beni. Spesso queste informazioni viaggiano sulla rete in chiaro e non in modalità protetta.
Un crescente numero di utenti, inoltre, sta fornendo un'elevata quantità di dati personali a social networks come MySpace, Facebook, chat, blog, ecc.
Ci sono poi delle tecniche specifiche di ingegneria sociale tramite internet, quali:

- **Phishing** - Questo termine identifica il furto di dati via mail. Il malvivente invia un'e-mail dichiarando di essere un incaricato di una banca o di una compagnia di carte di credito o di altre organizzazioni con cui si possono avere rapporti, richiedendo informazioni personali. Generalmente l'e-mail chiede di utilizzare un link per accedere ai dettagli del conto della vittima presso il sito della compagnia, adducendo

motivazioni di sicurezza, riscuotere premi in denaro, beni tecnologici, ripristinare password scadute, etc. Cliccando su quel link, tuttavia, l'utente sarà condotto in un sito web solo all'apparenza originale, in cui dovrà fornire informazioni private. I criminali potranno poi utilizzare i dati lasciati in tale sito fittizio per rubare denaro alle loro vittime.
- Questionari on line.
- Ingannare qualcuno a proposito della propria identità durante una chat, in un forum, ecc.
- **Finte promozioni o vincite**: mediante la ricezione di messaggi (SMS, Email) che, con la scusa di promozioni o vincite ad esempio di un telefonino di ultima generazione, portano a un link che porta ad una azione di phishing finalizzata ad acquisire i dati personali.

Ci sono comunque altri metodi, che non comportano l'utilizzo di internet, attraverso cui i criminali recuperano le informazioni necessarie per rubare l'identità:

- **Bin-raiding**. Documenti cartacei che non si ritiene importanti, come bollette del gas, della luce o del telefono, estratti conto e persino lettere personali e le buste in cui sono contenute, forniscono informazioni preziose che possono essere raccolte semplicemente rovistano nei rifiuti.
- **Contatti indesiderati.** Si deve fare molta attenzione a chi ci contatta, anche telefonicamente: spesso i truffatori si dichiarano incaricati di una banca o di un ente pubblico e vi chiedono di aggiornare i vostri dati personali. Accade la stessa cosa con coloro che si presentano come ricercatori di mercato e richiedono informazioni personali.
- **Furto o smarrimento del portafoglio**. Generalmente i portafogli contengono bancomat, carte di redito e documenti di identità come la patente di guida e le tessere di iscrizione a determinate associazioni.
- **Skimming**. Lo Skimming consiste generalmente nella clonazione di una carta di credito attraverso l'apparecchiatura elettronica utilizzata negli esercizi commerciali per pagare i beni acquistati. I dati che vengono raccolti, sono poi trasmessi a organizzazioni criminali.
- **Rubare l'identità di un deceduto**. I malviventi più spietati svolgono le loro attività criminali utilizzando l'identità di persone decedute, ottenendo informazioni sulla loro età, data di nascita ed indirizzo attraverso necrologi e pubblicazioni funebri.
- **Questionari cartacei**. Spesso vengono inviati per posta. Se sono molto lunghi, il compilatore non si accorge che sta fornendo a estranei delle informazioni private.
- **Tramite… noi stessi**. Capita, inconsciamente, di raccontare in pubblico fatti che ci riguardano (nell'anticamera del dottore, al supermercato durante la fila alla cassa, ecc.), non sapendo che per un ascoltatore interessato possono essere una miniera di dati.
- **Shoulder surfing** (letteralmente "fare surf alle spalle"). Designa quella semplice tecnica a metà tra l'informatica e il social engineering finalizzata all'impadronirsi di codici di accesso. Mentre la vittima digita la propria password (oppure il PIN o altri codici), il malintenzionato lo osserva, sia da vicino oppure anche da lontano (mediante lenti particolari o anche le riprese di telecamere a circuito chiuso), e riesce così ad

impossessarsi delle sequenze. Spesso ciò avviene tramite l'utilizzo di terminali POS oppure in luoghi molto frequentati, come ad esempio gli internet cafè.

Sono evidenti i motivi per cui è opportuno proteggere le proprie informazioni personali: se qualcuno entra in possesso di dati riservati, come le credenziali di accesso alla posta elettronica o a una rete sociale, ne può fare un uso illegale facendo ricadere la colpa su di noi (**furto di indentità**).

Domande

1. L'ingegneria sociale comprende solo tecniche informatiche online.
    a. Falso, comprende solo tecniche informatiche ma non online
    b. Falso, comprende solo tecniche online ma non informatiche
    c. Vero
    d. Falso
2. L'ingegneria sociale comprende:
    a. azioni telefoniche
    b. azioni con contatto "fisico"
    c. azioni on line
    d. tutte le risposte sono corrette
3. Quali delle seguenti tecniche non fa parte dell'ingegneria sociale?
    a. Pishing
    b. Dialer
    c. Shoulder surfing
    d. Telefonate

Per le risposte corrette vai all'ultima pagina del libro.

Capitolo 3

Sicurezza personale

Proteggere i dati

Misure per prevenire accessi non autorizzati ai dati

Abbiamo visto come sia essenziale proteggere i dati riservati, propri o altrui. Esistono, come vedremo più in dettaglio nei capitoli successivi, specifiche tecniche che possono essere applicate in **via preventiva**, per impedire l'accesso ai dati. Il metodo più usato è l'utilizzo di **Password**: sono stringhe di caratteri usate per l'autenticazione dell'utente, per dimostrare l'identità o ottenere l'accesso a una risorsa.

Nel campo della sicurezza informatica, si definisce autenticazione il processo tramite il quale un computer, un software o un utente, verifica la corretta, o almeno presunta, identità di un altro computer, software o utente che vuole comunicare attraverso una connessione.

La forma di autenticazione più semplice si fonda sull'utilizzo di un **nome utente** (per *identificare* l'utente)e di una **password** (o parola d'ordine, per *autenticare* l'utente).

L'autenticazione tramite nome utente è password è ormai molto diffusa nell'ambiente delle reti e di internet: per accedere alla propria postazione di lavoro in una rete aziendale o addirittura al proprio pc, per accedere alla posta elettronica in remoto, per le operazioni di home banking, per accedere a servizi di messaggistica istantanea, ecc. è sempre necessaria l'autenticazione.

Il motivo è ovvio. Il sistema a cui si vuole accedere deve essere sicuro che l'utente è proprio quello che ne ha il diritto.

Se per il nome utente non ci sono raccomandazioni particolari, può essere un nome di fantasia semplice da ricordare, la password deve essere scelta in modo oculato, **non deve essere comunicata ad altre persone** e, in casi di dati riservati o importanti, **deve essere cambiata con regolarità.**

Come deve essere una password?

La password deve essere lunga a sufficienza, composta da lettere e numeri e non facilmente associabile alla vita dell'utente: quindi non il proprio nome, cognome, soprannome, data di nascita, indirizzo, ecc.

Ci sono tecniche che impediscono l'utilizzo dei dati se, nonostante le misure preventive, qualcuno sia venuto in possesso di queste informazioni. La **Crittografia** analizza come "offuscare" un messaggio in modo che non sia comprensibile a persone non autorizzate a leggerlo.



Un tale messaggio si chiama **crittogramma** e le tecniche usate per rendere incomprensibile il messaggio si chiamano tecniche di **cifratura**. La crittografia è utilizzata in tutti gli ambiti dove è necessaria la segretezza delle informazioni: informazioni militari (soprattutto in caso di conflitti), informazioni bancarie riservate, comunicazioni tra Stati, spionaggio, ecc. Esistono metodi di crittografia molto sofisticati per l'importanza dei dati che devono trattare. Un esempio (molto semplice) di tecnica crittografica è il disco cifrante di Leon Battista Alberti, che per primo insegnò a cifrare per mezzo di un con un alfabeto segreto che si ottiene spostando il disco interno di due o tre parole.



Caratteristiche fondamentali della sicurezza delle informazioni

Riassumendo, i dati personali e/o riservati per essere sicuri, devono avere un alto fattore di **confidenzialità**, cioè devono essere protette da accessi o divulgazione non autorizzati.
Queste protezioni non devono comunque essere di ostacolo all'**integrità** dell'informazione, la quale deve essere affidabile cioè integra, completa, senza modifiche rispetto all'originale.
È fondamentale poi la **disponibilità** dell'informazione al momento del bisogno: non avrebbe senso esasperare la sicurezza dei dati se poi, quando servono, per qualche motivo non si riesce a recuperarli nei tempi necessari.

Principali requisiti per la protezione, conservazione e controllo di dati/privacy che si applicano in Italia

Nel gennaio 2012, la Commissione Europea ha approvato la proposta di un regolamento sulla protezione dei dati personali, in sostituzione della direttiva 95/46/CE valida per i 27 stati membri dell'Unione Europea e una direttiva che disciplina i trattamenti per finalità di giustizia e di polizia (attualmente esclusi dal campo di applicazione della direttiva 95/46/CE).

In accordo con questo regolamento sulla protezione dei dati personali in Italia è stato emesso Decreto Legislativo n. 5 del 9 febbraio 2012 che ha preso il posto del precedente Dlgs 196/2003.

Il decreto contiene un articolato pacchetto di interventi volto ad alleggerire il carico degli oneri burocratici gravanti sui cittadini e sulle imprese, con una semplificazione delle procedure amministrative, ad esempio per il cambio di residenza, comunicazioni di dati tra le amministrazioni, partecipazione a concorsi, ecc.

Importanza di creare e attenersi a linee guida e politiche per l'uso dell'ICT.

Vista l'importanza dell'argomento, ci sono delle specifiche linee guida e politiche per l'uso dell'ICT, delle regole chiare che forniscono uno standard che deve essere seguito dagli utenti e disciplinano l'utilizzo delle tecnologie informatiche e delle telecomunicazioni (ICT) per preservare i dati, personali e aziendali, dal furto, dallo smarrimento e da un utilizzo non consentito. Assicurano una posizione chiara su come dovrebbe essere usata l'ICT per assicurare la protezione dei dati aziendali. In questo modo le aziende (come i privati) possono tutelarsi e devono, a loro volta, tutelare i propri dipendenti, clienti e fornitori.

Alcune di queste linee sono:

- Non lasciare che i dettagli dei principali conti aziendali siano di pubblico dominio, così che i frodatori possano ottenere dettagli sufficienti per intaccarli.
- Predisporre un'accurata politica di gestione e archiviazione dei documenti: è il primo passo per proteggere l'azienda e i dipendenti contro il furto di identità.
- Distruggete tutti i documenti riportanti dati sensibili: le aziende hanno il dovere di conservare e proteggere le informazioni dei propri clienti e dei propri dipendenti oltre che l'obbligo. Abbiamo visto che in Italia è in vigore il Decreto Legislativo n. 5 del 9 febbraio 2012 che dichiara che "chiunque per motivi professionali conserva o tratta dati sensibili altrui (e quindi, tutte le organizzazioni, le aziende, gli enti pubblici, i professionisti …) è soggetto alle cautele e agli obblighi previsti dalla legge in quanto responsabile civilmente e penalmente anche in modo oggettivo di ogni danno cagionato al titolare o a terzi da un trattamento non corretto; il trattamento dei dati è considerato un' attività pericolosa e come tale gode dell'inversione dell'onere della prova (art. 2050 Codice Civile): è il responsabile del trattamento dei dati che ha l'onere di dimostrare il corretto utilizzo per evitare di incorrere in sanzioni civili e penali. L'ufficio del Garante della Privacy può richiedere alle autorità di polizia di effettuare controlli e le sanzioni per il mancato rispetto della legge possono arrivare a 80.000 euro (articoli da 161 a 172 del decreto). La legge elenca 17 possibili operazioni di trattamento dei dati. In particolare, i dati su supporti cartacei o multimediali una volta cessato il trattamento devono essere distrutti

(art. 16, c. 1-a). Distruggere i supporti, cartacei e non, è infatti il modo migliore per evitare che i criminali possano avere accesso ai dati sensibili.

- Mettere i dipendenti a conoscenza dei rischi di frode di identità aziendale: questo può garantire che rimarranno vigili.
- Assicurarsi che la procedura di gestione dei documenti sia comunicata e correttamente eseguita da tutti i dipendenti. Fare in modo che siano cauti nel fornire le informazioni dell'azienda on-line o via telefono, verificando con chi effettivamente hanno a che fare.
- Assicurarsi che il sistema operativo antivirus e firewall (che vedremo nei capitoli successivi) siano tenuti aggiornati. In questo modo i dipendenti possono aprire in sicurezza gli allegati delle e-mail ricevute.

Domande

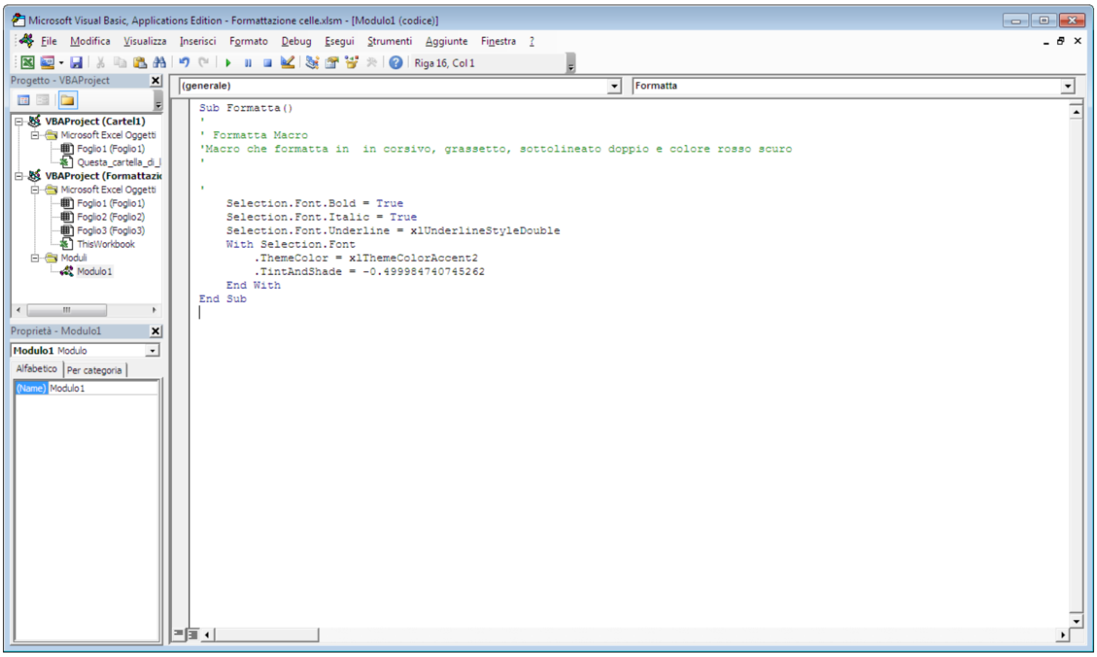
1. Il regolamento sulla protezione dei dati personali in Italia è
    a. Il Decreto Legislativo n. 5 del 9 febbraio 2012
    b. Dlgs 196/2003
    c. Direttiva 95/46/CE
    d. Nessuno dei precedenti
2. Con "Disponibilità dei dati" si garantisce l'assenza di modifiche non autorizzate nel file
    a. No, è la possibilità di accedere ai dati
    b. È corretto
    c. Dipende dal tipo di dati
    d. No, garantisce l'assenza di modifiche autorizzate
3. Una password, per essere efficace, deve essere formata da una combinazione di lettere, numeri e caratteri speciali.
    a. No, solo lettere
    b. No, solo numeri
    c. No, solo caratteri speciali
    d. È vero
4. I dipendenti di una azienda devono essere messi a conoscenza dei rischi di frode di identità aziendale.
    a. È falso
    b. È vero
    c. Solo i quadri dirigenziali
    d. Solo gli addetti ai terminali

Capitolo 4

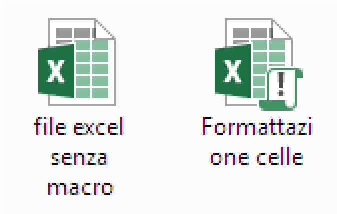
Sicurezza dei file

Le protezioni nei programmi

Attivare/disattivare le impostazioni di sicurezza delle macro.
Una macro è un insieme d’istruzioni che il computer interpreta una dopo l’altra e traduce in azioni operative, né più né meno come se fossero state impartite manualmente da noi. Una macro può essere eseguita indefinitamente tutte volte che si desidera, e pertanto si rivela una ottima soluzione per automatizzare una volta per tutte l’esecuzione di procedure ricorrenti. Le applicazioni pratiche delle macro sono solo da immaginare**:** la stampa di una tabella, la formattazione di un documento, la creazione di un grafico, la ricerca di particolari valori, ecc.
Le macro, nel caso delle applicazioni Microsoft Office come Word, Excel, Access, sono scritte nel linguaggio Visual Basic for Application (VBA).

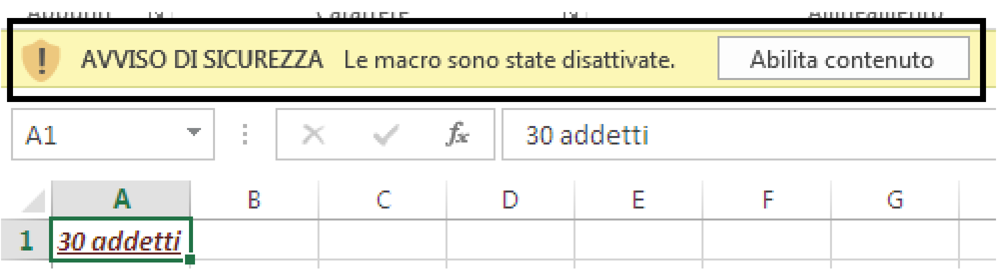


La sua funzione è quella di rendere programmabili questi applicativi, allo scopo di personalizzarli a seconda delle esigenze specifiche dell'utente.
Le macro generate per un file sono parte integrante del file. Il sistema operativo Windows visualizza l’icona dei file con macro in modo diverso dagli altri. Hanno un punto esclamativo che le contraddistingue e un’estensione diversa (xlsm).

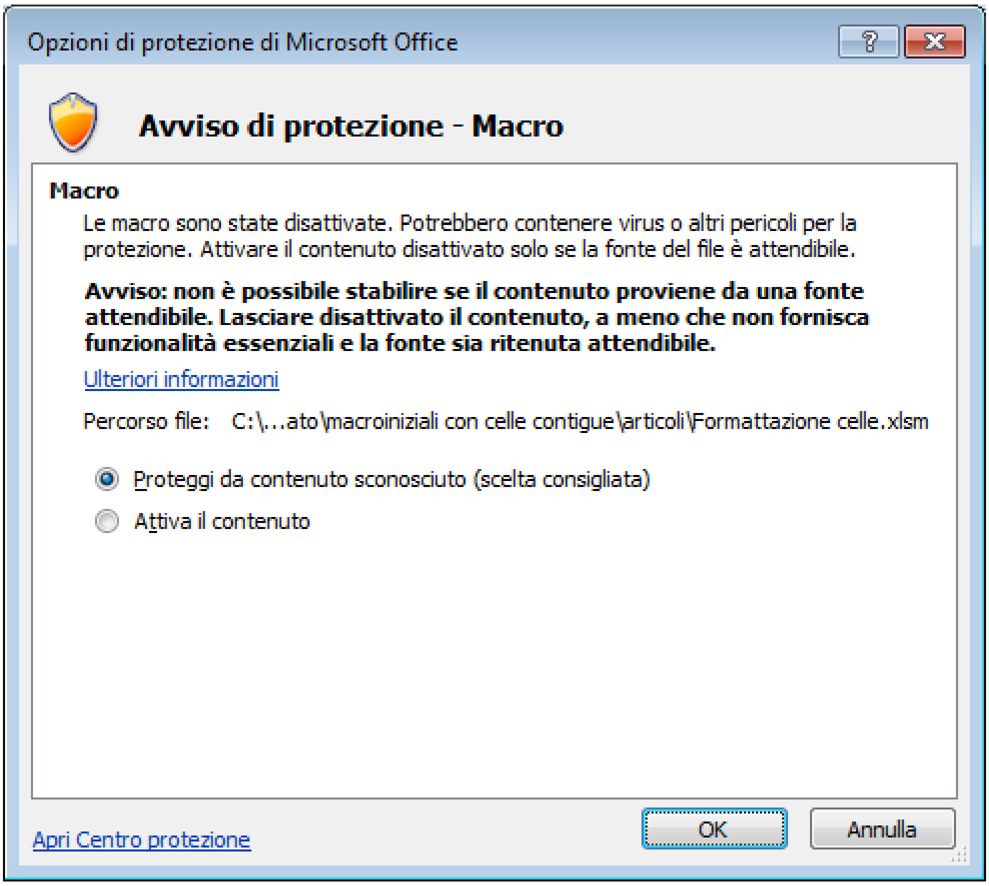


Aprire un file contenente delle macro

Abbiamo già visto che l'icona di un file con macro presenta un punto esclamativo, per porre attenzione sulla diversità rispetto ai file "normali".
Quando si apre un file con macro il programma ci avvisa della presenza di questo codice con un *avviso di protezione* nella barra di notifica.



I programmi Office, per impostazione predefinita, disattivano le macro presenti in un file. È una questione di sicurezza. Non conoscendo a priori il contenuto delle macro presenti, se sono "sicure" o se è codice "pericoloso" (per questo l'icona del file ha il segnale di attenzione) scritto per creare dei danni, si decide di disabilitare il codice.
Se si è sicuri del contenuto della macro, ad esempio perché è stata scritta dal proprietario del file, si può abilitare il codice con il pulsante **Opzioni**.

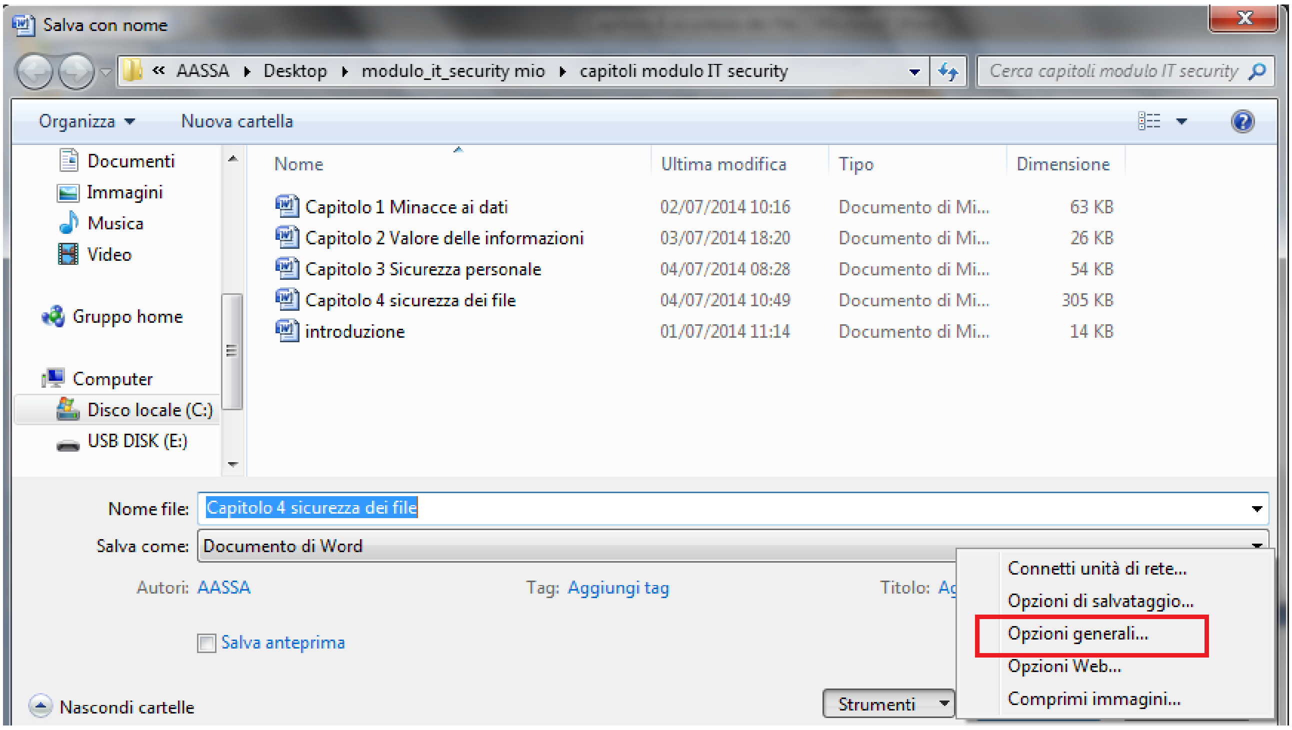


Le macro abilitate possono essere eseguite, Chiaramente, nel caso di macro di provenienza non nota o se l'autore delle macro non è attendibile, questa esecuzione potrebbe comportare dei danni al computer.

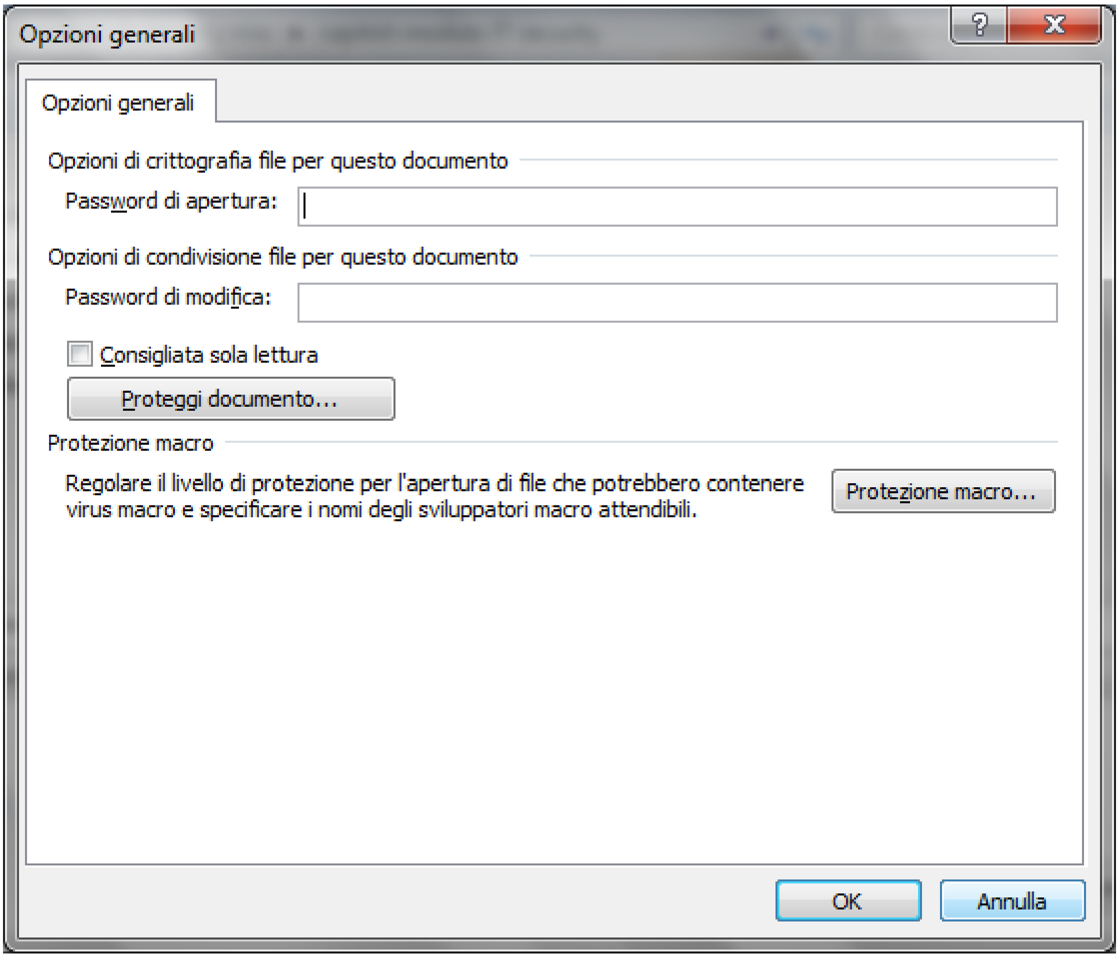
Impostare una password per file quali Documenti e/o fogli di calcolo

È possibile proteggere un documento o un foglio di calcolo dall'apertura e/o dalla modifica mediante una password. Abbiamo già visto, nei capitoli precedenti, le caratteristiche che deve avere una password. Aggiungendo a un documento una password di apertura non sarà possibile aprirlo se non si digita la password corretta. Aggiungendo una password di modifica sarà possibile aprire il documento senza digitare la password, ma esso verrà aperto in sola lettura.

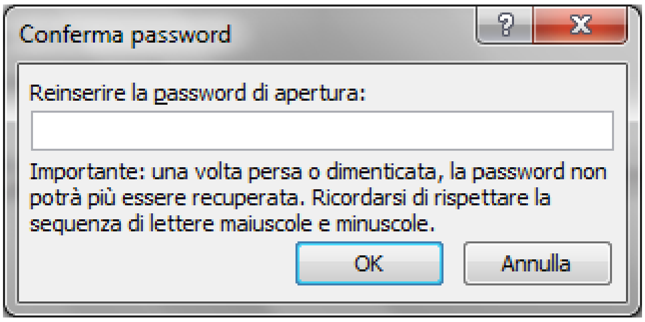
Per aggiungere una protezione mediante password a un documento o foglio di calcolo, per i programmi Microsoft Office, dal pulsante Office (versione 2007) o dal menu **File** (per la versione 2010), si sceglie il comando **Salva**, o **Salva con nome** se il documento era già stato salvato in precedenza.



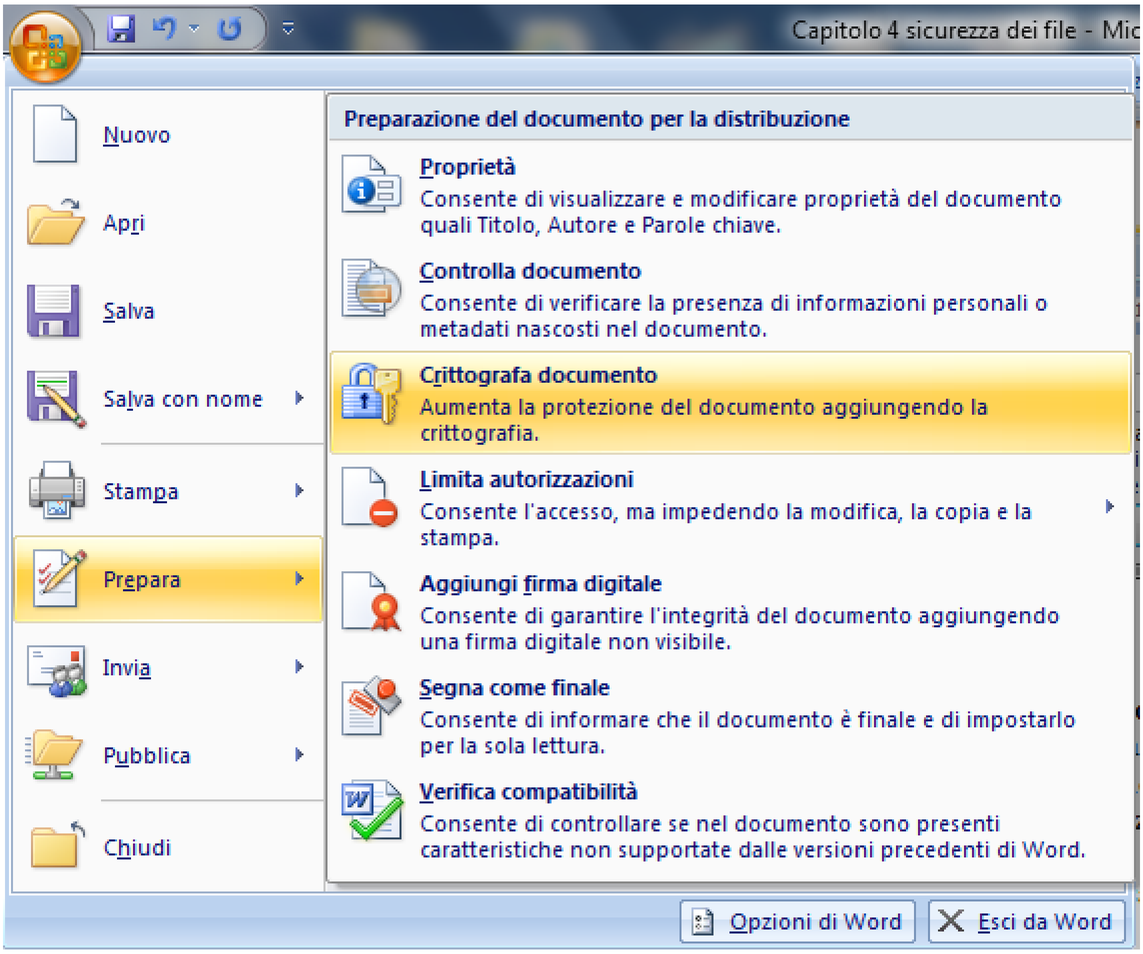
Dal menu **Strumenti**, selezionare la voce **Opzioni generali**. Appare la finestra per impostare le password di apertura e di modifica.



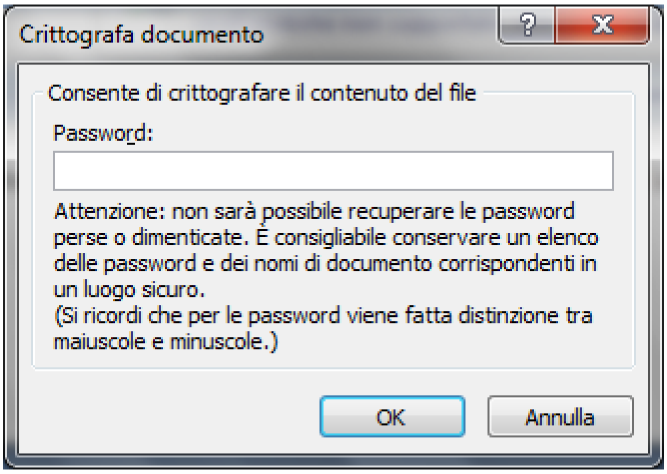
A questo punto si può digitare una password di apertura e/o una password di modifica del documento. Verrà richiesta la conferma delle password.



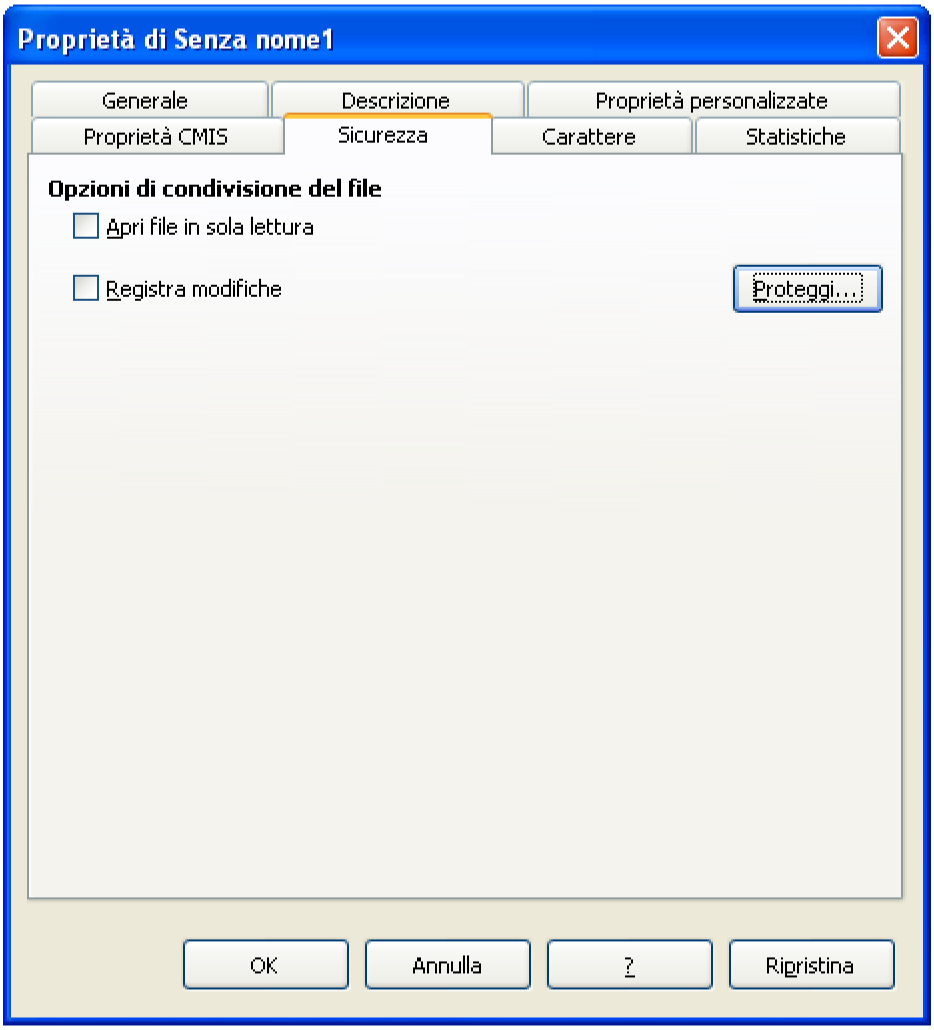
Eventualmente, si può selezionare la casella **Consigliata sola lettura**: in questo modo all'apertura del documento verrà visualizzato un messaggio che ne consiglia l'apertura in sola lettura. Se si modifica il documento aperto in sola lettura, sarà necessario salvarlo con un nome diverso. È possibile selezionare la casella **Consigliata sola lettura** senza impostare alcuna password.
Altre impostazioni di protezione sono presenti nel pulsante Office con la voce **Prepara**.



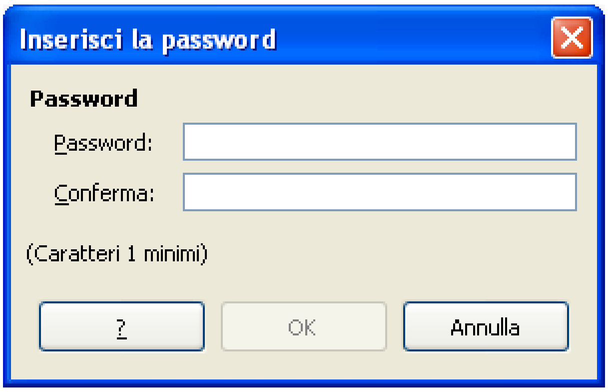
Scegliendo la voce **Crittografa documento** appare la finestra per inserire la password.



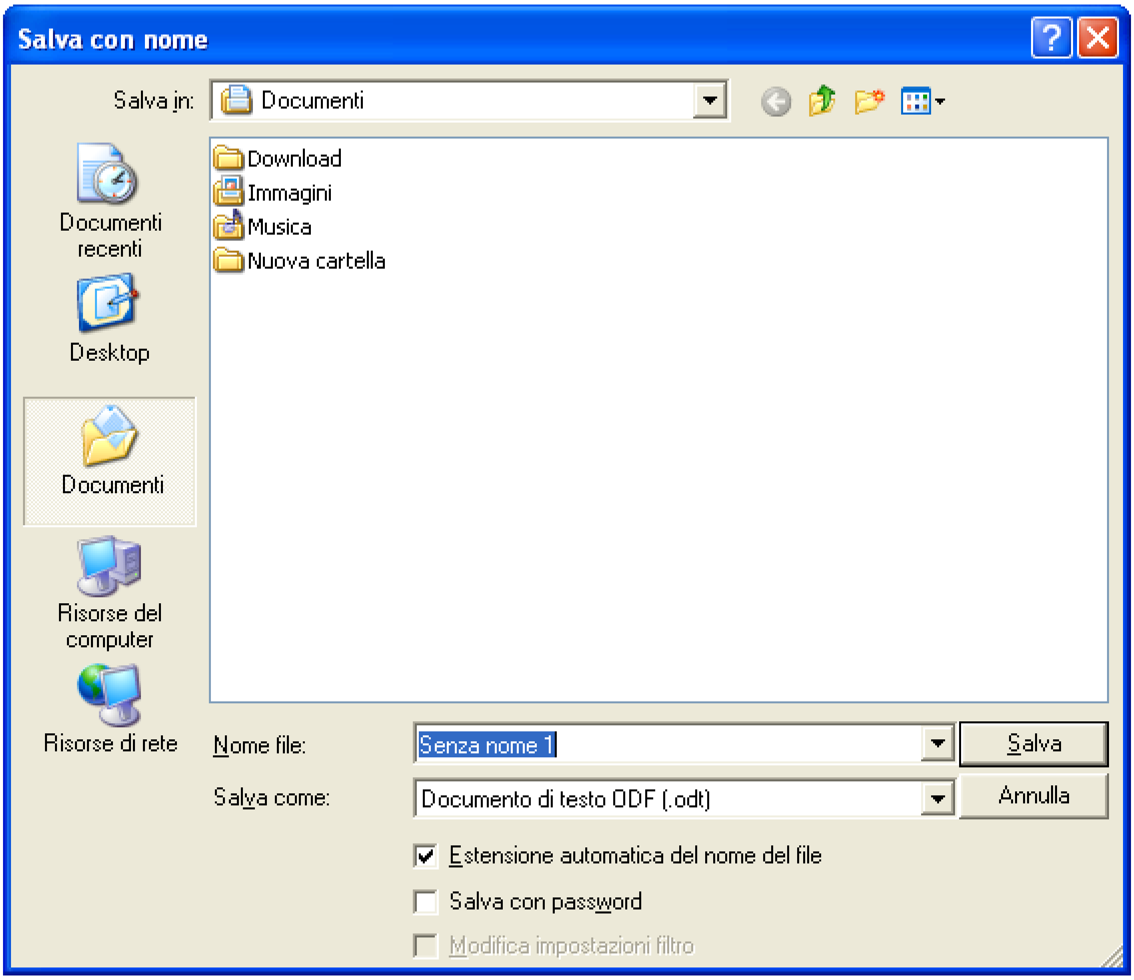
Il documento protetto da password viene crittografato con specifiche tecniche in modo che sia illeggibile da chi non è in possesso del codice di accesso.
Nel caso di software libero, come Libreoffice, la procedura per proteggere un documento è simile. Una volta aperto il file da proteggere, si sceglie **Proprietà** dal menu **File**.



Nella scheda **Sicurezza** fare clic sul pulsante **Proteggi**.



A questo punto si può inserire e confermare la password da applicare. Si può impostare la protezione con password anche con il comando **Salva con nome**.

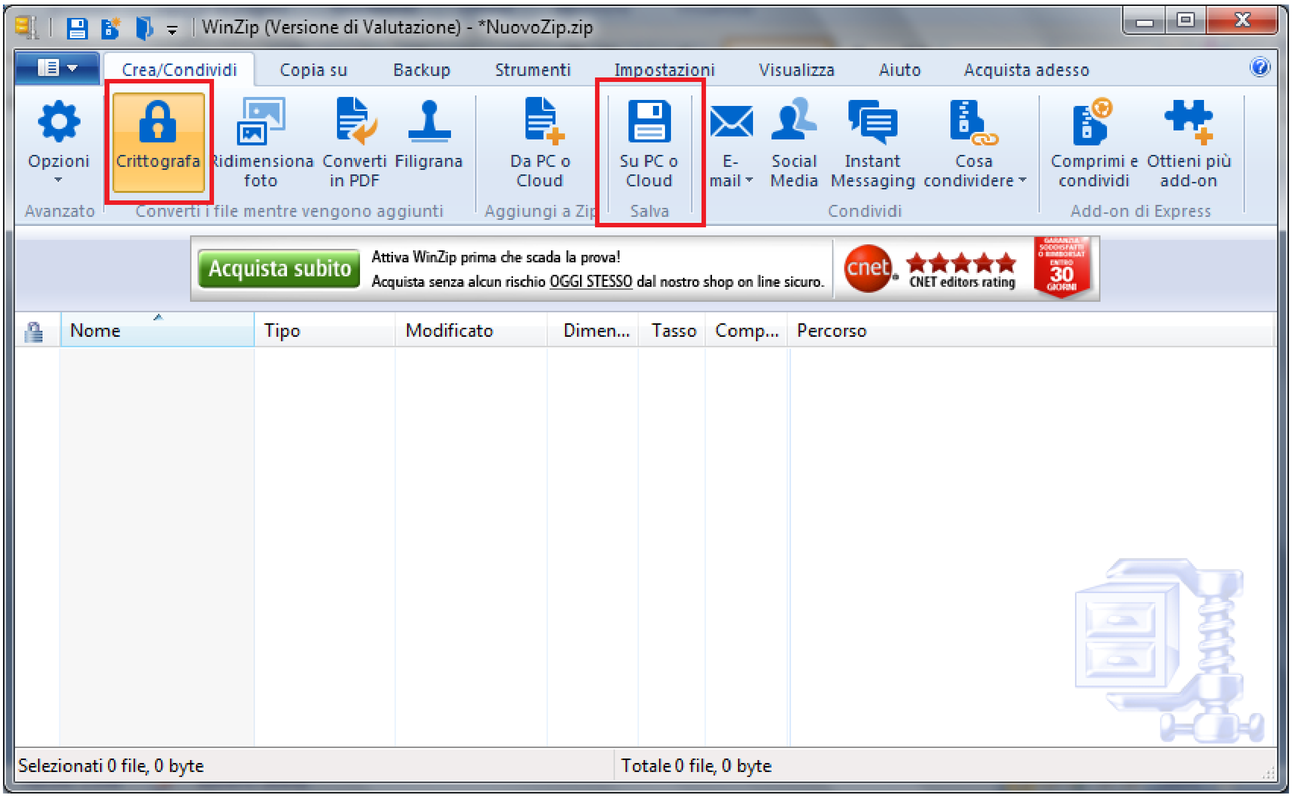


Impostare una password per file compressi

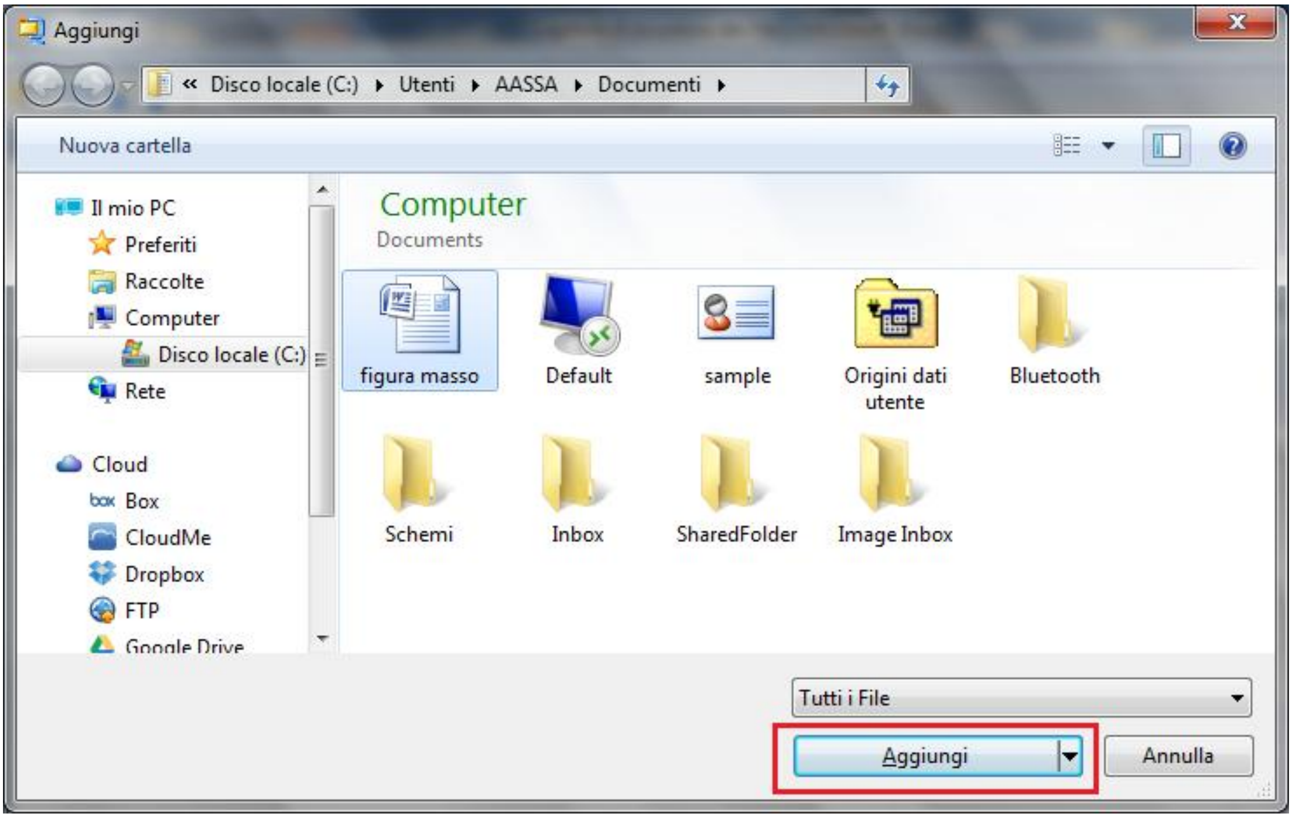
I programmi di compressione permettono, tramite opportune tecniche, di ridurre le dimensioni dei file.

Esistono vari programmi di questo tipo come WinZip, WinRar,Tar.Gz, ecc.

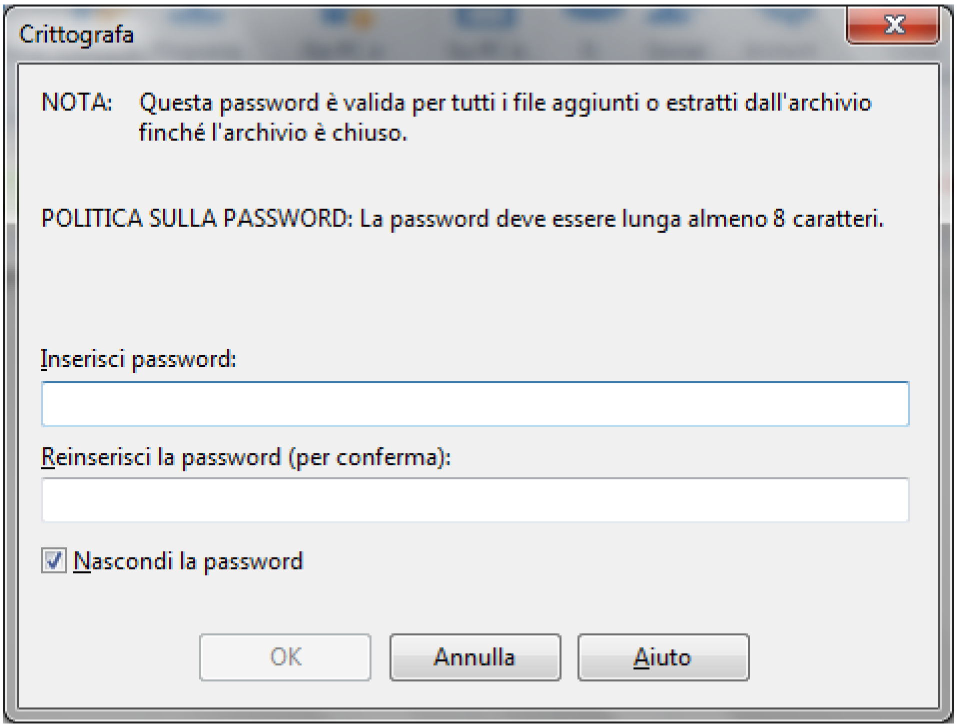
Nel programma WinZip, nella versione dotata di funzioni di cifratura, selezionare **Crittografa** nella scheda **Crea/Condividi**.



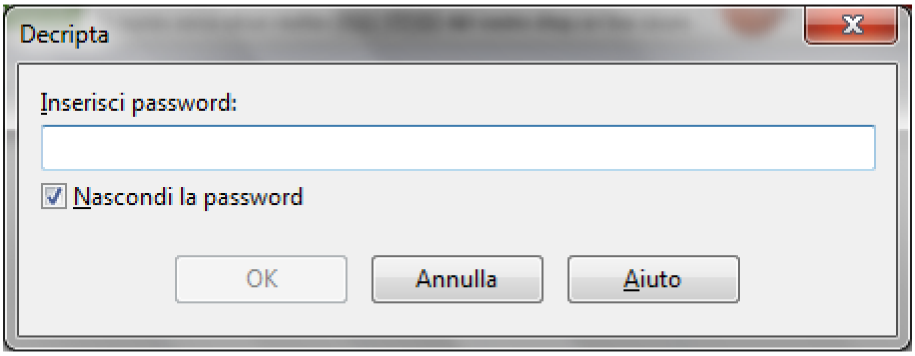
Sempre nella scheda Crea/Condividi fare clic sul pulsante **Da Pc o Cloud** per aggiungere a WinZip i file da comprimere.



Fare clic su **Aggiungi**. Dopo un avviso relativo ai vantaggi e svantaggi dei metodi di crittografia, appare la finestra per inserire la password.



Scegliere una password e reinserirla una seconda volta. Fare clic su **OK**. Quando si apre il file compresso appare la finestra di richiesta della password per decriptare il file.



Vantaggi e i limiti della cifratura.

Se si protegge un documento, un foglio di calcolo, un file compresso con una password, per riaprire il documento è necessario fornire la password corretta. I dati cifrati non possono essere letti senza la chiave d'accesso e solo il proprietario o il destinatario autorizzato del file può leggere il messaggio.
Chiaramente è fondamentale che la password sia conservata dal proprietario in modo sicuro e che possa essere facilmente ritrovata dallo stesso in caso di bisogno.
La sicurezza dei dati protetti attraverso la crittografia dipende non solo sulla forza del metodo di crittografia, ma anche sulla forza della propria password, compresi fattori quali la lunghezza e la composizione della password e le misure che si prendono per assicurarsi che la password non sono comunicati a terzi non autorizzati.

Domande

1. In MS Excel, nell’estensione dei file tipo “xlsm”, la lettera m significa:
    a. Minimum
    b. Macro
    c. Mega
    d. Micro
2. Qual è l’estensione per un file compresso
    a. Zip
    b. Rar
    c. Tar.Gz
    d. Tutte le risposte sono corrette
3. In Ms Word è possibile impostare una password:
    a. Solo di apertura
    b. Solo di modifica
    c. Solo per la cifratura
    d. Di apertura, di modifica e di cifratura

Capitolo 5

Malware

Definizione e funzione

Cos'è un Malware

Il termine *Malware* è l'abbreviazione di "malicious software", software dannoso. Malware è un qualsiasi tipo di software indesiderato che viene installato senza un adeguato consenso. Lo scopo di un malware è creare danni al software (e hardware) del computer o ai dati dell'utente del pc: rovinare un sistema operativo, compromettere funzioni del computer, compiere, all'insaputa dell'utente, azioni illegittime con il computer (ad esempio, inviare e-mail dall'account di posta del pc o attaccare altri computer), prelevare o danneggiare i dati, modificare le connessioni, raccogliere vari tipi d'informazioni personali, installare software all'insaputa, e reindirizzare ad altre pagine internet indesiderate, ecc.
Spesso si confonde il termine malware con *virus*. Per malware si intende l'intera tipologia dei software dannosi. Un virus è un *tipo di malware* che, come vedremo, ha la caratteristica di *replicarsi* infettando l'intero computer e quelli a cui sono collegati: un virus, per infettare il pc, *necessita dell'intervento umano* come il doppio clic di mouse su un file o su un'immagine in internet. Da quel momento darà inizio al contagio.
Un malware si può introdurre in un computer in vari modi. In generale i malware si diffondono tra i pc sfruttando i metodi di comunicazione esistenti. Ogni sistema adatto a trasportare informazioni da un pc a un altro è candidato a diventare sistema di infezione. È possibile infettare un computer attraverso una chiave USB, un cd o ogni altro strumento di memorizzazione rimovibile, oppure utilizzando le reti informatiche.
Attualmente i malware si diffondono soprattutto utilizzando le reti di computer, prima tra tutti internet, e la posta elettronica, sfruttando anche l'inesperienza di molti utenti e, nel caso delle mail, la curiosità. Gli utenti devono prestare attenzione soprattutto quando scaricano file e programmi da internet, soprattutto da siti poco conosciuti, e alle e-mail con allegati. Proprio le e-mail sono il metodo di diffusione principale dei malware, sfruttando "buchi" dei software di posta e la curiosità degli utenti che aprono qualsiasi messaggio arrivi sul PC, anche da indirizzi sconosciuti.

Diversi modi con cui si può nascondere il malware

Abbiamo visto che un malware si può introdurre in un computer in diversi modi. A seconda dei casi si può distinguere in:
Trojan: chiamato anche Trojan Horse, consiste in un file nascosto all'interno di programmi di utilizzo comune e largo utilizzo. Per esempio, si potrebbe trovare un gioco gratuito disponibile in rete che, una volta scaricato ed eseguito, senza che l'utente stesso ne sia a conoscenza, avvia e installa il codice trojan nascosto nel programma: questo codice lavora in background nel sistema con lo scopo di danneggiarlo oppure di rubare informazioni. È

chiamato “Cavallo di Troia” proprio perché nasconde secondi fini, dove apparentemente non vi è nessun rischio.
Rootkit: il termine si può tradurre come “equipaggiamento per amministratore”. È un insieme o un singolo software capace di controllare un computer locale o remoto, nascondendosi. In questo modo un hacker può accedere e impossessarsi del computer di un utente e usarlo per i suoi scopi: rubare i dati, utilizzare il computer per attaccare altri sistemi, ecc.
I rootkit attaccano i moduli più interni del sistema operativo, spesso per nascondere delle *backdoors* (porte di servizio, vedi definizione successiva) per scavalcare le porte di sicurezza attivate da un sistema informatico o da un pc, entrando nel sistema.
Non sempre un rootkit è un software maligno. Può essere “regolare” come parte di un software legittimo, ad esempio per il controllo remoto di un pc da parte di un centro di assistenza.
Backdoor: le backdoor (letteralmente”porta sul retro”) consentono di superare le procedure di sicurezza, attivate dal sistema informatico o computer, per entrare nel sistema. Queste porte possono essere create per agevolare la manutenzione o il controllo remoto del pc da utenti autorizzati. Si pensi al caso di un centro assistenza di una software house che opera in remoto per adeguare on line un programma acquistato presso di loro. In questo caso le backdoors sono usufruite in maniera corretta. Invece, se sono installate automaticamente da malware, permettono l’ingresso di utenti malintenzionati che possono utilizzare il pc con il controllo remoto senza che il proprietario ne sappia nulla.

Malware infettivo

Un malware infettivo è composto da poche righe di codice che si attaccano a un programma, infettandolo. Si installa automaticamente e lavora in background.
Il malware infettivo consiste, in linea di massima, di virus e worm.
Virus: un virus è un programma che si attiva e si diffonde in modo totalmente indipendente dalla volontà dell'utente.
L'obiettivo è quello di danneggiare i dati o i programmi dei destinatari, oppure infettare altre applicazioni, modificandole e includendovi una copia di se stessi. Si usa il termine "virus" in quanto il suo comportamento può essere paragonato a quello biologico, per la similitudine del modo di propagarsi dell'infezione.
In genere i virus si “nascondono” per un certo tempo e durante questo periodo, chiamato “letargo”, controllano tutti gli eventi del sistema operativo o quelli legati all'utente. Quando si verifica l'evento atteso, per esempio viene aperto un determinato file, il virus inizia la sua azione.
La “vita” di un virus informatico si svolge in tre fasi: trasmissione, riproduzione e alterazione.

1. Nella fase di trasmissione il virus “infetta” uno o più file del computer;
2. nella fase di riproduzione il virus copia se stesso nel sistema, all'interno del singolo PC o nella rete.
3. Nella fase di alterazione il virus svolge il suo compito, che spesso significa danneggiare dati e programmi.

Worm: tradotto in lingua italiana “Verme“. Questo tipo di malware modifica il sistema operativo in modo da essere eseguito automaticamente ogni volta che viene acceso il

sistema, rimanendo attivo per tutta la durata di tempo, fin quando non si spegne il computer. Si muove quindi senza bisogno di intervento esterno. È in grado di replicarsi come fa un virus, ma non ha bisogno di "attaccarsi" ad altri file eseguibili dato che usa internet per potersi riprodurre rapidamente. Uno dei mezzi per il contagio è la posta elettronica: il worm invia email ai contatti memorizzati allegando un file infetto (Attachment).

Malware usati per furto di dati, profitto/estorsione

Abbiamo visto che un malware può essere progettato con lo scopo di creare danni alle componenti software e hardware del computer su cui viene eseguito. Ma ci sono malware creati per avere un profitto in modo più o meno illecito. Tra questi ci sono:

Adware: (abbreviazione di *advertising-supported software*, "Software sovvenzionato da pubblicità"). È un programma che propone messaggi pubblicitari, non richiesti dall'utente, attraverso finestre popup o durante il processo di installazione di un software. L'apertura di continui popup pubblicitari può rallentare le prestazioni del computer. Altri adware modificano le pagine html proposte dal browser per includere link e messaggi pubblicitari propri. Molti adware inoltre comunicano le abitudini di navigazione dell'utente a server remoti, violando la privacy.

Spyware: ("software spia"). Uno spyware non attacca il computer per danneggiarli, ma, durante l'attività al pc, raccoglie e trasferisce dati e informazioni dell'utente del pc. Questi dati possono essere strettamente personali e riservati, come password, numero di carta di credito, ecc., ma anche indicazioni sull'attività del proprietario del computer: ad esempio, acquisti online, siti visitati, chiaramente senza il consenso. Le informazioni sono vendute ad aziende per effettuare della pubblicità mirata.

Botnet: letteralmente tradotto significa "rete di bot". *Bot* è un'abbreviazione di "robot", ma il termine che rende più l'idea di questo tipo di infezione è "zombie". Attraverso falle nella sicurezza o per mancanza di attenzione da parte dell'utente, il dispositivo viene infettato per consentire ad hacker malintenzionati (*botmaster*) di controllare il sistema da remoto: in questo modo il computer può iniziare a svolgere operazioni a insaputa del proprietario: si può far parte di una botnet senza neanche saperlo. Più computer infettati e controllati formano una *botnet*: se un computer diventa parte di una botnet, potrebbe rallentare ed essere completamente in balia di hacker.

Chi è in possesso di una botnet può far svolgere qualsiasi azione ad ogni singolo computer infetto: inviare messaggi email indesiderati, diffondere virus, attaccare "in massa" computer e server. Infatti, una botnet è formata da un numero elevato di computer, addirittura milioni di pc. Con un tale "esercito" si può sferrare un attacco in sincronia (*DDos*, Distributed Denial Of Service) contro server di enti, società governative, aziende e multinazionali.

Keylogger: un keylogger è uno strumento capace di registrare tutto quello che un utente digita sul suo computer. Dispositivi di keylogger possono essere presenti anche nei bancomat per intercettare il codice PIN. I keylogger possono essere di tipo hardware, inserito dentro la tastiera o collegato al cavo tra tastiera e pc, o software.

Dialer: è un programma che si auto installa nel computer e modifica i parametri della connessione internet e impostarla verso numeri telefonici molto costosi. L'utente si troverà di fronte a inspiegabili aumenti delle bollette telefoniche. Chi utilizza una linea ADSL non corre alcun rischio dato che non è prevista la connessione remota.

Domande

1. Il termine malware e virus sono sinonimi
    a. È vero
    b. Un virus non è un malware
    c. Un virus è un tipo di malware che per attivarsi necessita dell'intervento umano
    d. Un virus è un tipo di malware autonomo
2. Quale delle seguenti indicazioni sui rootkit è corretta?
    a. I rootkit sono sempre dannosi
    b. I rootkit non sono sempre dannosi
    c. I rootkit sono delle particolari macro
    d. I rootkit si nascondono sempre in altri programmi
3. Tutti i malware sono progettati per danneggiare i computer che infettano
    a. È falso
    b. È vero
    c. Solo i Worm
    d. Solo i Dialer
4. Qual è un software autonomo e dannoso che non si attacca ad altri programmi
    a. Trojan
    b. Worm
    c. Spyware
    d. Tutte le risposte sono errate
5. Quale può essere un veicolo di virus?
    a. Allegato a una mail
    b. File scaricato dal Web
    c. Pendrive USB
    d. Tutte le risposte sono corrette
6. Quale estensione può riferirsi a un file potenzialmente pericoloso?
    a. Exe
    b. Bat
    c. Com
    d. Tutte le estensioni citate

Capitolo 6

Proteggersi dai malware

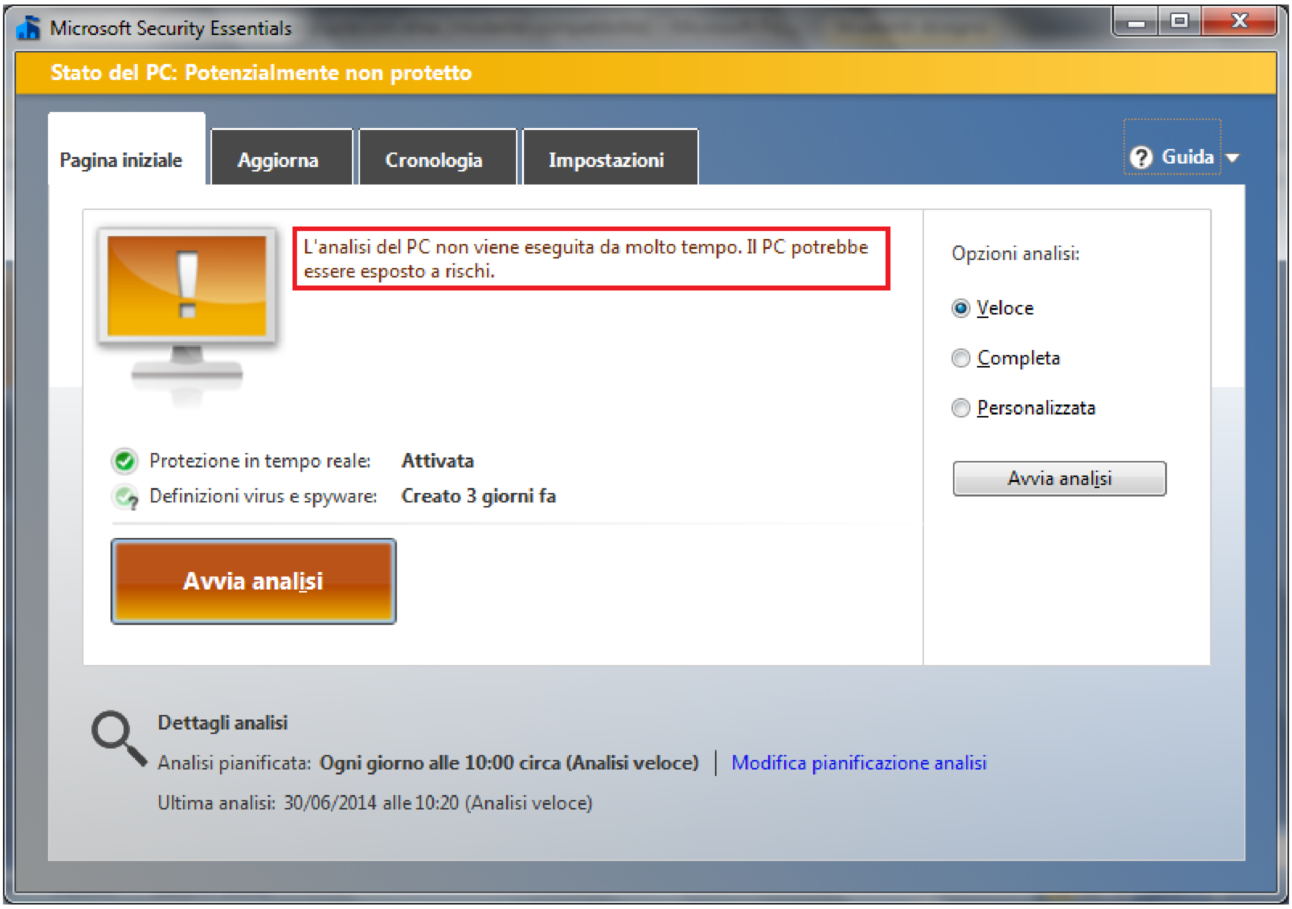
Antivirus e antimalware

Un antivirus è anche antimalware?

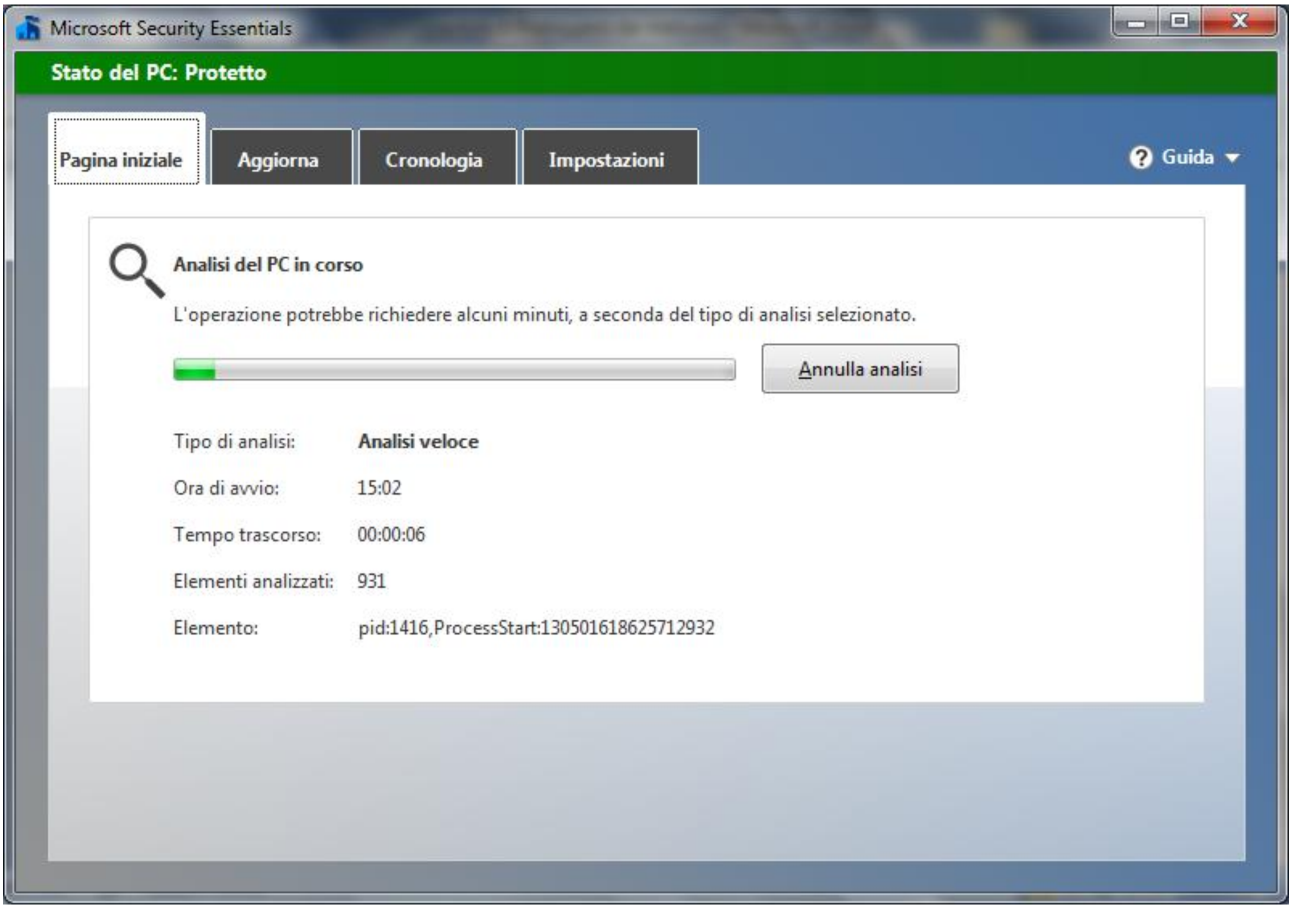
Nel capitolo precedente abbiamo visto come nel computer si può introdurre, all'insaputa dell'utente, del software con lo scopo di provocare un danno. Questi programmi sono detti malware e un virus è una delle tipologie di malware. La caratteristica che contraddistingue un virus è la capacità di replicarsi automaticamente e diffondersi nel computer proprio come un virus biologico.
Dato che i virus, e i danni che hanno creato, hanno fatto molto clamore, spesso si identificano i due termini.
Per combattere il software maligno le aziende produttrici di software per la sicurezza hanno creato dei programmi appositi: gli *antivirus* e *antimalware*. Diciamo subito che ora come ora non c'è una distinzione tra i due prodotti. Normalmente è sottointeso che un programma antivirus è anche antimalware: nella descrizione del prodotto è indicato da quali tipologie di intrusione protegge. Per la maggior "fama" del termine virus si usa genericamente il termine antivirus.
Non si può avere una protezione totale contro i virus, per la continua evoluzione del software maligno, ma è possibile limitare al minimo il rischio di infezione con un buon programma antivirus. A volte può capitare che, per "eccesso di zelo", un antivirus segnali come pericoloso un file totalmente innocuo ("falsi positivi"), ad esempio per la presenza di macro costruite dall'utente.
In generale gli antivirus hanno un sistema di protezione *real time*: operano una *scansione* continua mentre si naviga nel web, quando si installano delle applicazioni e quando si apre un file. Ma, come vedremo, può essere avviata una scansione manuale o periodica per assicurarsi che nulla sia trascurato.

Fare una scansione con un software antivirus

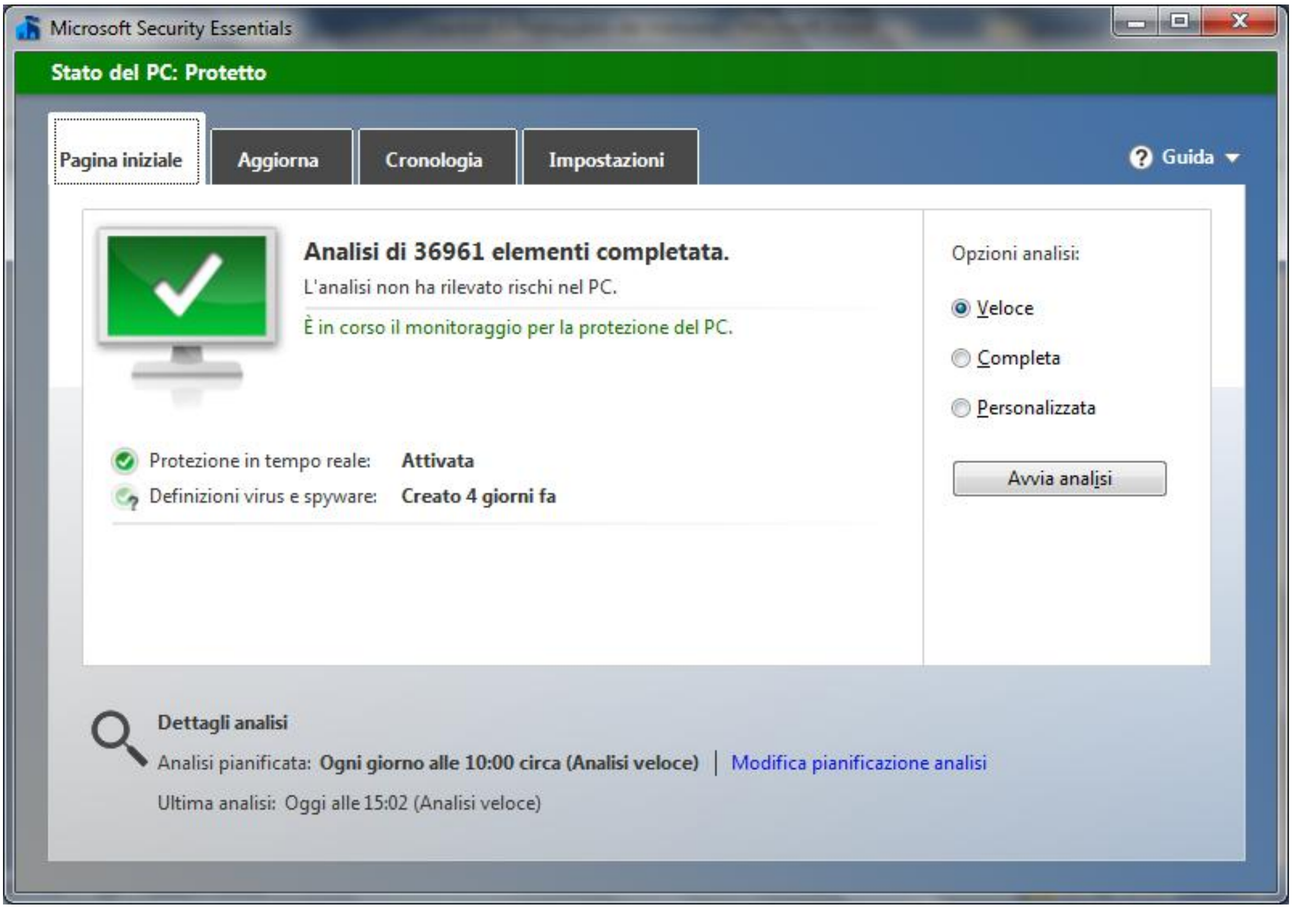
Esistono tanti antivirus, gratuiti o a pagamento, con diversi livelli di sicurezza e affidabilità. A volte è offerta una versione base gratuita con la possibilità di ottenere, a pagamento, il programma completo di tutte le potenzialità. Tutti prevedono la possibilità di effettuare una scansione manuale del software presente nel computer per la ricerca di virus.
In questo manuale utilizziamo il software Microsoft Security Essential (MSE). I comandi per gli altri tipi di antivirus sono comunque molto simili.
Una volta avviato il programma, appare la finestra principale di MSE.



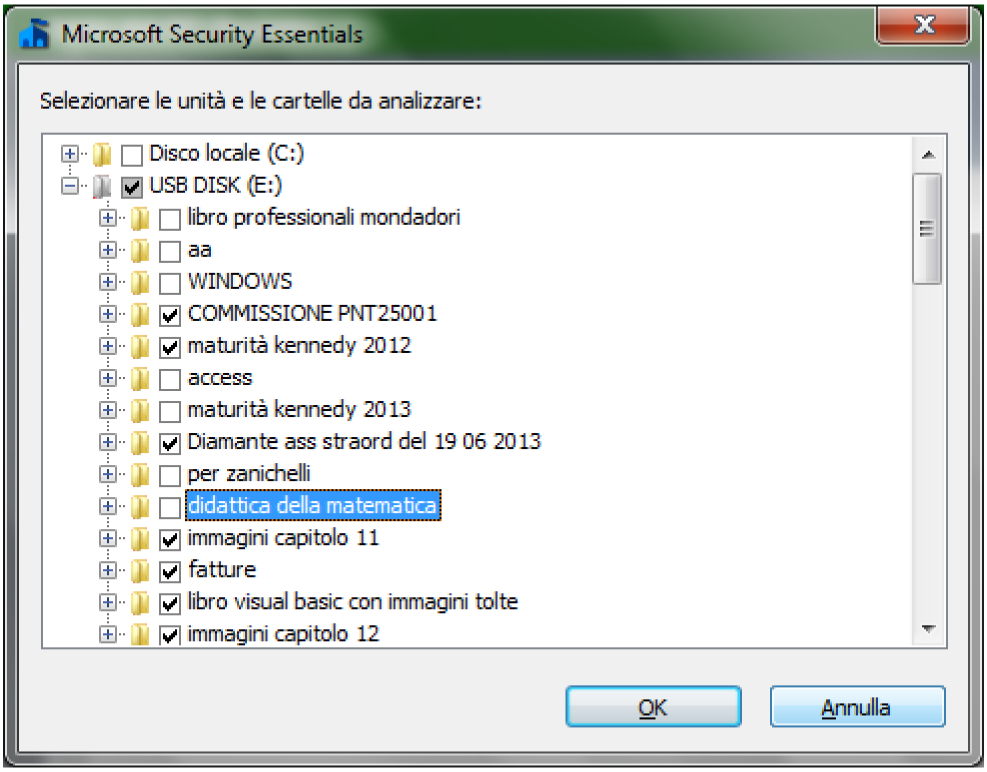
Da qui si possono avviare tutte le operazioni. In figura, il programma segnala che è da molto tempo che non viene effettuata una scansione manuale.
Per avviare la scansione premere il pulsante **Avvia analisi**.



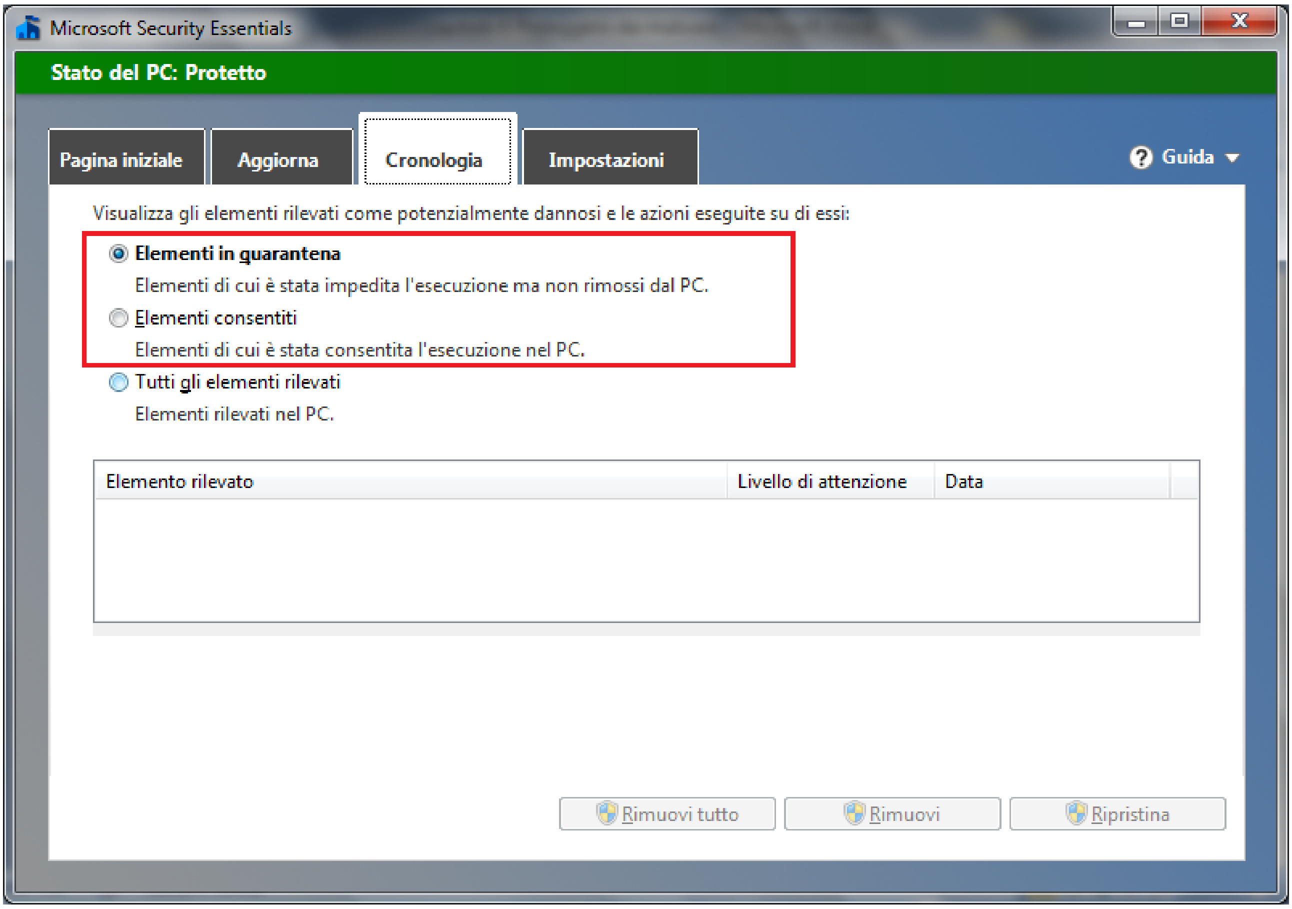
Al termine del processo, se non sono stati rilevati malware, appare il riepilogo degli elementi controllati.



Ci sono tre tipi di scansione: con la scansione **Veloce** i virus sono cercati nei punti dove si nascondono più di frequente. Se si pensa che il computer sia infetto, nonostante la scansione veloce non abbia dato esito, si può eseguire la scansione **Completa**. In questo caso verranno controllati tutti i file del disco rigido e i programmi in esecuzione. Questo processo può durare alcune ore e le prestazioni del computer saranno rallentate. La scansione **Personalizzata** permette all’utente di scegliere i file da esaminare.

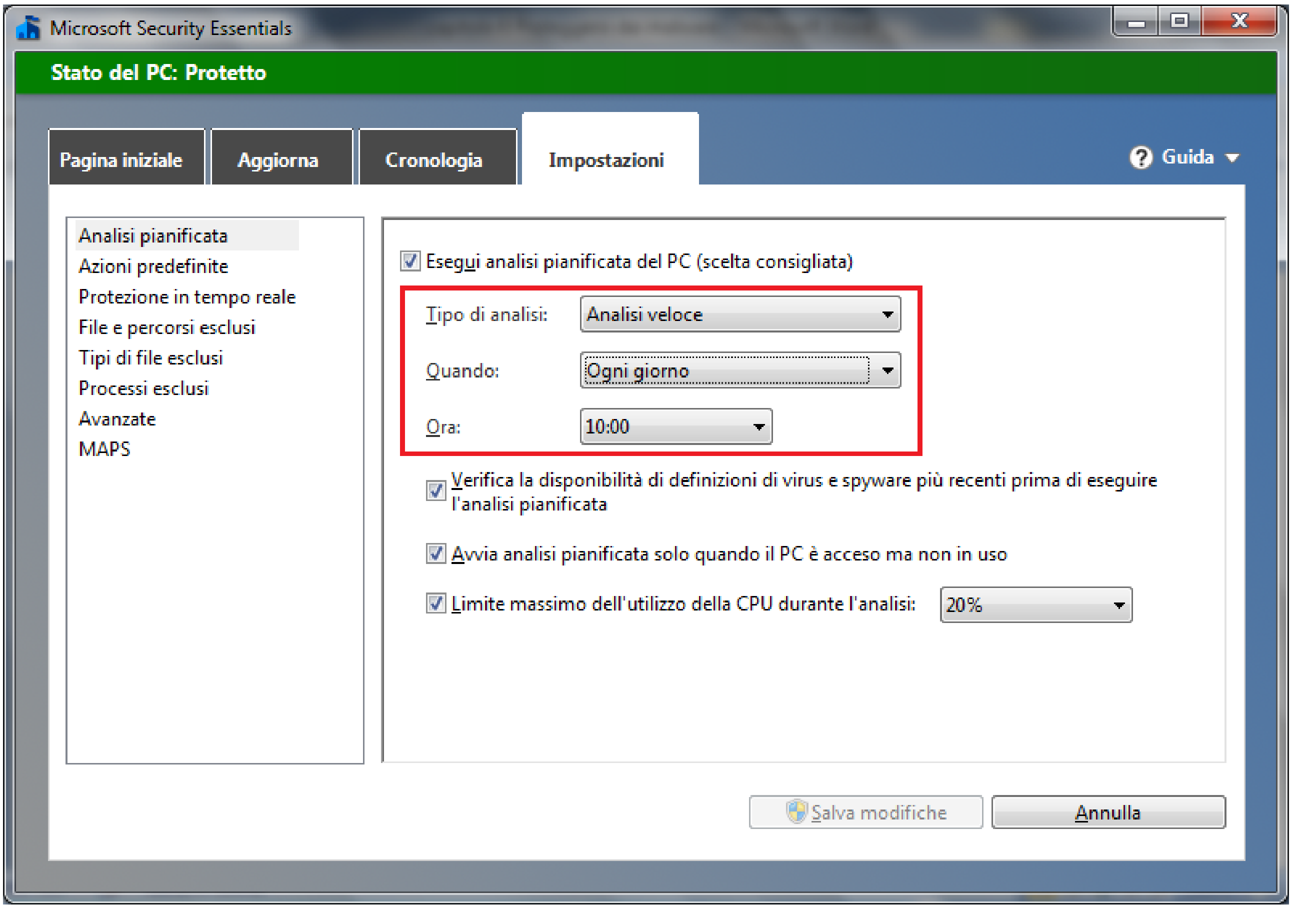


Se l’antivirus rileva del software dannoso, il più delle volte, interviene automaticamente per rimuoverlo e invia un messaggio di notifica all’utente. In altri casi MSE segnala la presenza di software potenzialmente pericoloso e lascia all’utente la scelta dell’azione da intraprendere.
L’utente può *rimuovere* il file o *consentire* la sua presenza. Può, in alternativa, mettere l’elemento in **quarantena**. Il file viene spostato in un’altra posizione nel computer e non verrà eseguito fino a quando non verrà consentito o rimosso. I file in quarantena e consentiti, per MSE, sono visibili nella scheda **Cronologia**.



Pianificare le scansioni

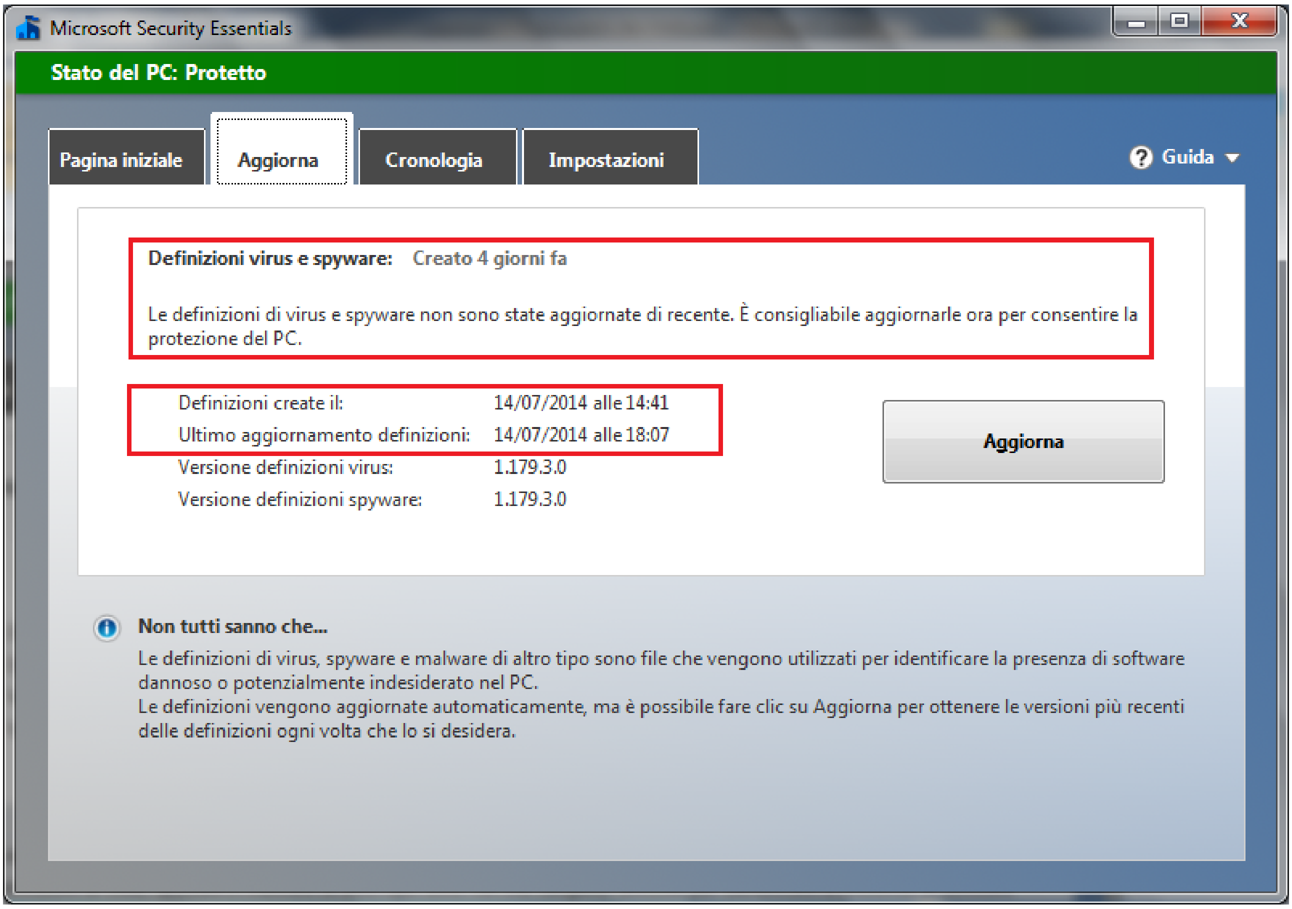
La scansione dei file può essere impostata in modo che sia eseguita automaticamente nelle date e nell'orario stabiliti dall'utente. In MSE, nella scheda **Impostazioni**, si può scegliere il tipo di analisi, la giornata e l'orario.



Aggiornare l'antivirus

Ogni giorno vengono creati nuovi malware. Di conseguenza i produttori di software antivirus *aggiornano* le *definizioni* di questi programmi dannosi. Le definizioni di virus, spyware e altri tipi di malware non sono altro che dei file che sono utilizzati dal programma antivirus per rilevare il software dannoso.

MSE, nella finestra iniziale e nella scheda **Aggiorna**, segnala all'utente da quanto tempo non procede con gli aggiornamenti e permette di scaricarli con un clic su **Aggiorna**.



È importantissimo aggiornare con una certa frequenza l'antivirus per avere il computer protetto dalle nuove minacce. Per questo motivo, gli antivirus attuali prevedono l'aggiornamento in automatico.

Domande

1. In genere è possibile pianificare una scansione antivirus
    a. È falso
    b. È possibile solo con gli antivirus commerciali
    c. È possibile solo con gli antivirus gratuiti
    d. È vero
2. Il software antivirus non necessita di aggiornamenti
    a. Falso
    b. Un antivirus non si aggiorna
    c. Gli aggiornamenti non sono importanti
    d. Solo nel caso di sistema operativo Linux
3. Un file identificato come infetto dall'antivirus deve essere eliminato subito perché sicuramente dannoso. Non esistono "Falsi positivi"
    a. È sempre vero
    b. È sempre falso
    c. Può capitare questo tipo di casi
    d. Tutte le risposte sono errate
4. Cosa si può fare con un file segnalato dall'antivirus come infetto ma sospettato "falso positivo"?
    a. Fare una ricerca online per avere maggiori informazioni sul file
    b. Cancellarlo in ogni caso
    c. Non cancellarlo mai, è un errore dell'antivirus
    d. Tutte le risposte sono errate
5. Cosa significa che un file è in quarantena
    a. Che non è infetto
    b. Che non è stato controllato dall'antivirus
    c. Che è un file di backup
    d. Che non verrà eseguito fino a quando non verrà consentito o rimosso
6. Il verbo inglese "to download" significa:
    a. scaricare
    b. cancellare
    c. duplicare
    d. caricare

Capitolo 7

Le reti

Sicurezza in rete

Tipi di reti

Con il termine *rete* si intende un insieme di componenti, sistemi o entità interconnessi tra loro. Nell'ambito dell'informatica, una rete è un complesso sistema di connessione di dispositivi informatici attraverso collegamenti fisici (linee telefoniche, cavi dedicati, onde radio, ecc.) al fine di utilizzare nel miglior modo possibile le risorse disponibili e di offrire vari servizi di comunicazione.

Il progetto di una rete copre ampie problematiche che vanno della sua architettura fisica alla codifica dei dati per facilitare la trasmissione, fino alla costruzione del software applicativo che mette a disposizione degli utenti i servizi di rete.

Negli ultimi due decenni, grazie alla rapida evoluzione delle tecnologie telematiche, c'è stata una espansione frenetica delle reti sia a livello locale (nelle aziende e negli uffici), sia a livello mondiale (Internet).

I principali vantaggi di una rete sono:

1. Condivisione risorse (file, periferiche…)
2. Indipendenza dei singoli elaboratori
3. Tolleranza ai guasti
4. Dischi e servizi di backup
5. Condivisione delle informazioni
6. Possibilità di lavoro di gruppo

In base all'estensione, geografica si possono identificare i seguenti tipi di reti.

Una rete locale o **LAN** (Local Area Network) è un gruppo di elaboratori e di altri dispositivi elettronici interconnessi che si trovano all'interno dello stesso edificio ed utilizzano mezzi trasmissivi dedicati e privati. Una normale LAN è quindi una *piccola* rete (da 2 a 30 utenti), che comunque non attraversa il suolo pubblico con i propri mezzi trasmissivi; ciò esonera il sistema dal puntuale rispetto degli standard della telefonia e della trasmissione dei dati pubblici.

Quando la rete locale diventa fisicamente molto grande e le distanze fra gli elaboratori aumentano considerevolmente, vengono inseriti nella struttura della rete dei dispositivi (quali *hub*, *bridge* o *switch*) che consentono di potenziare il segnale che fluisce attraverso i cavi in modo che raggiunga in maniera comprensibile il destinatario. Una rete formata da nodi che si trovano a notevoli distanze e che utilizzi canali trasmissivi che attraversano il suolo pubblico viene detta **WAN** (*Wide Area Network*): è una rete molto estesa a livello geografico, fino a livello mondiale come la rete internet.

Le problematiche di una WAN sono molto diverse di quelle di una LAN sia a causa dei vincoli imposti dagli enti preposti al controllo delle telecomunicazioni, sia per i diversi mezzi trasmissivi che il messaggio deve attraversare prima di giungere al destinatario.
Nelle reti geografiche vengono usati tutti i mezzi trasmissivi disponibili, dai doppini telefonici alle fibre ottiche, utilizzando anche le più moderne tecnologie satellitari.
A metà via tra LAN e WAN si trovano le reti **MAN** (*Metropolitan Area Network*) che utilizzano tecnologie simili a quelle delle reti locali, avendo però mezzi trasmissivi messi a disposizione da un gestore pubblico. In effetti una WAN è formata dalla connessione di un elevato numero di elaboratori singoli, reti locali e MAN e la sua efficienza si misura nel modo in cui permette la comunicazione fra le varie reti di base.
Un "ibrido" tra una Lan e una Man sono le reti **VPN** (Virtual Private Network). Una VPN è una rete privata (caratteristica della LAN) che sfrutta una rete pubblica (caratteristica della MAN e WAN), la rete internet, per permettere ai computer appartenenti alla rete di comunicare tra loro come se fossero collegati allo stesso server. Il termine "Virtuale" è dovuto al fatto che i computer non sono effettivamente collegati solo tra loro, non hanno delle linee dedicate, ma utilizzano una struttura pubblica quale, appunto, la rete internet. La rete VPN permette a computer ubicati in luoghi fisici diversi di stabilire un collegamento privato come se ci fosse un "tunnel" virtuale che corre tra i nodi pubblici di internet.
Dato che le connessioni a internet sono connessioni pubbliche, quindi con accesso non protetto, c'è il rischio che le informazioni trasmesse sul web attraverso una VPN possano essere intercettate. Per questo motivo con una rete VPN è possibile crittografare i dati e inviarli solo a un computer, o a gruppi di computer specifici. Inoltre i collegamenti attraverso le reti VPN necessitano di una *autenticazione* all'accesso, in modo che l'utilizzo sia concesso solo a utenti autorizzati. La sicurezza è quindi garantita dai protocolli di cifratura e dall'autenticazione.

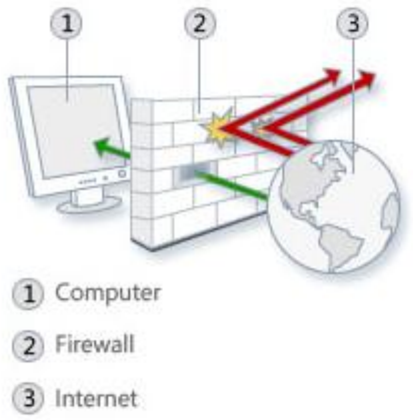
L'amministratore di rete

Abbiamo visto come, nell'utilizzo di una rete, sia di fondamentale importanza garantire la sicurezza dei dati e l'accesso ad essi solo da parte di utenti autorizzati.
L'*amministratore di rete* (o di sistema) è la figura professionale che, oltre ad occuparsi della gestione e della manutenzione della rete, deve garantire, anche per aspetti "legali", un'adeguata protezione dei dati. Non sono amministratori di sistema coloro che intervengono sugli elaboratori solo occasionalmente (per esempio, a scopo di manutenzione straordinaria).
L'individuazione precisa e responsabile di tali soggetti è una delle scelte fondamentali all'interno di un'azienda. Infatti, l'amministratore di sistema deve implementare, in raccordo con il titolare e/o eventuali altri responsabili delle informazioni, *politiche di accesso* alle risorse della rete, come documenti, cartelle, componenti hardware, ecc. Deve stabilire chi, e come, può accedere alle risorse del sistema informativo e a tutti i dati personali aziendali (anche sensibili): per tale motivo gli amministratori di sistema devono essere scelti con particolare attenzione, poiché i rischi che possono correre le banche dati o le reti informatiche sono sempre più elevati.
La gestione degli accesi avviene con l'assegnazione di *account*, composto da un nome utente e una password, agli utenti del sistema. Il nome utente serve a identificare l'utente, la password ad autenticare. Ad ogni account è associato il rispettivo livello di abilitazione per l'accesso alle risorse.

L’amministratore deve aver cura di conservare l’elenco degli account in un luogo sicuro e richiedere la modifica periodica delle password da parte degli utenti.

Firewall

Un firewall (letteralmente, muro di fuoco) è un software, o un hardware, se non addirittura un computer o un insieme di computer posto sul “confine” telematico, ad esempio presso il modem o il router, tra un computer, o una rete locale, e il resto del mondo collegato alla rete. Serve per proteggere contro aggressioni provenienti dall’esterno e blocca eventuali programmi presenti sul computer che tentano di accedere ad internet senza il controllo dell’utente. Il firewall applica dei filtri software ai dati in entrata e in uscita, per bloccare gli attacchi via internet.



Configurare il firewall di Windows: consentire un programma

Per garantire il controllo in entrata e in uscita, un firewall deve essere ben configurato. La sua configurazione è un compromesso tra usabilità della rete, sicurezza e risorse disponibili per la manutenzione della configurazione stessa Le regole che si impostano per il firewall influenzano l’efficace funzionamento.

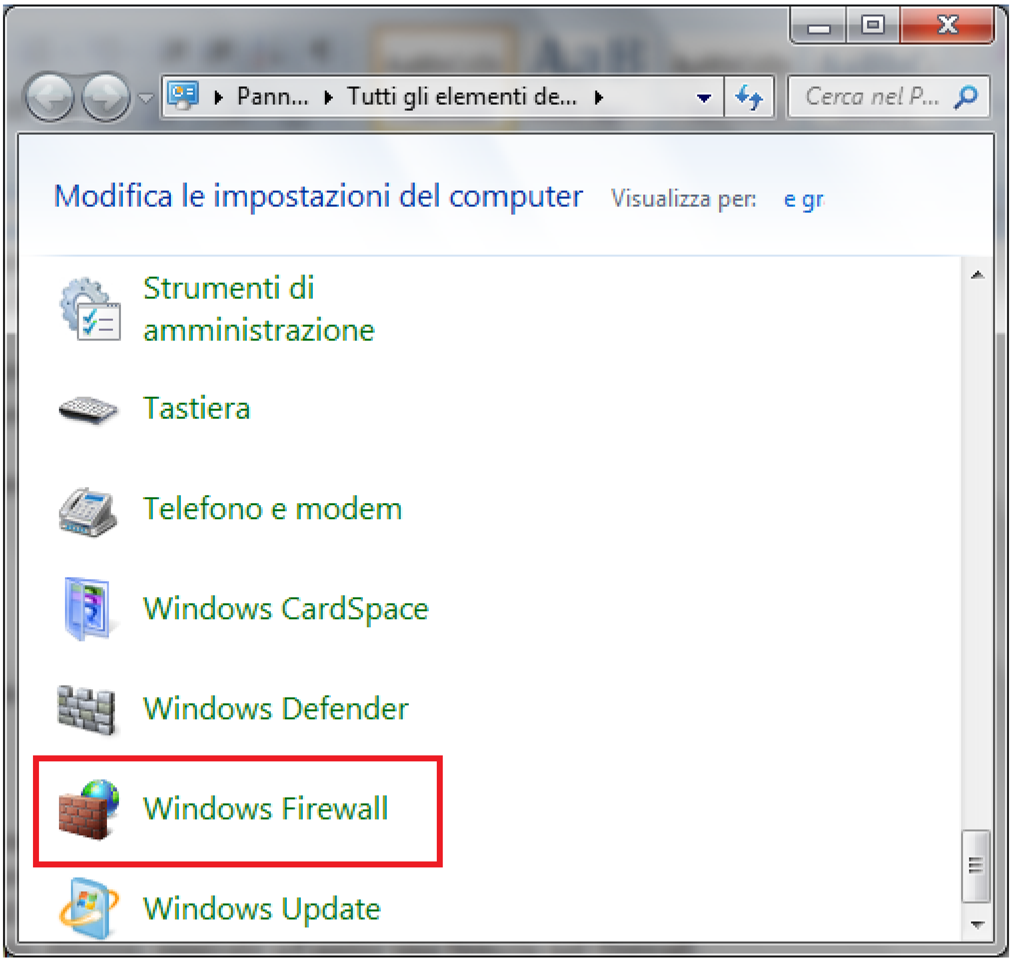
Il firewall presente in Windows consente di specificare quali programmi possono ricevere informazioni attraverso il firewall e di impostare regole per le connessioni in entrata e in uscita.

Per prima cosa vediamo come consentire ad un programma di inviare o ricevere informazioni attraverso il firewall.

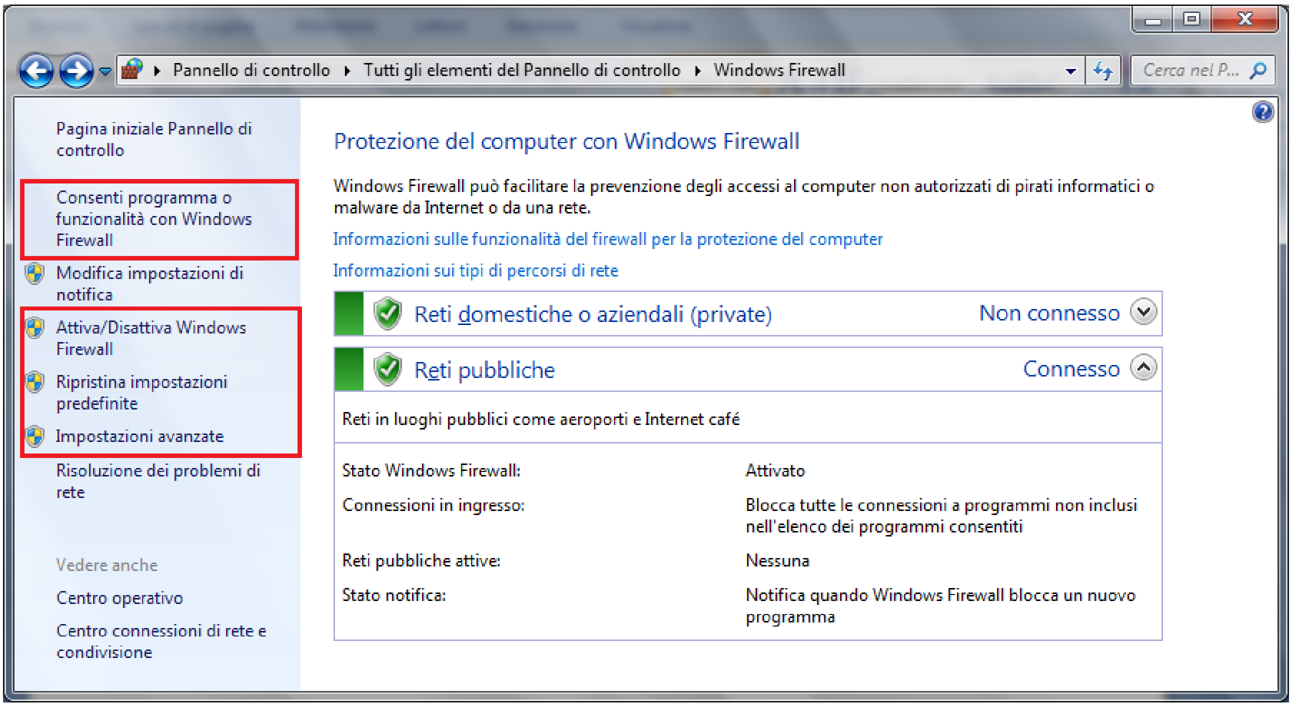
Per impostazione predefinita, la maggior parte dei programmi viene bloccata da Windows Firewall per garantire una maggiore sicurezza del computer. Ma potrebbe essere necessario consentire a tali programmi di comunicare attraverso il firewall.

Ad esempio, proviamo ad aggiungere ai programmi consentiti alla comunicazione il browser Mozilla Firefox. Può capitare che il firewall non consente la connessione con Firefox: in questo caso, il browser può riportare errori di tipo “Indirizzo non trovato” quando si cerca di accedere ad un sito web.

Per accedere al firewall aprire il **Pannello di controllo** di Windows.

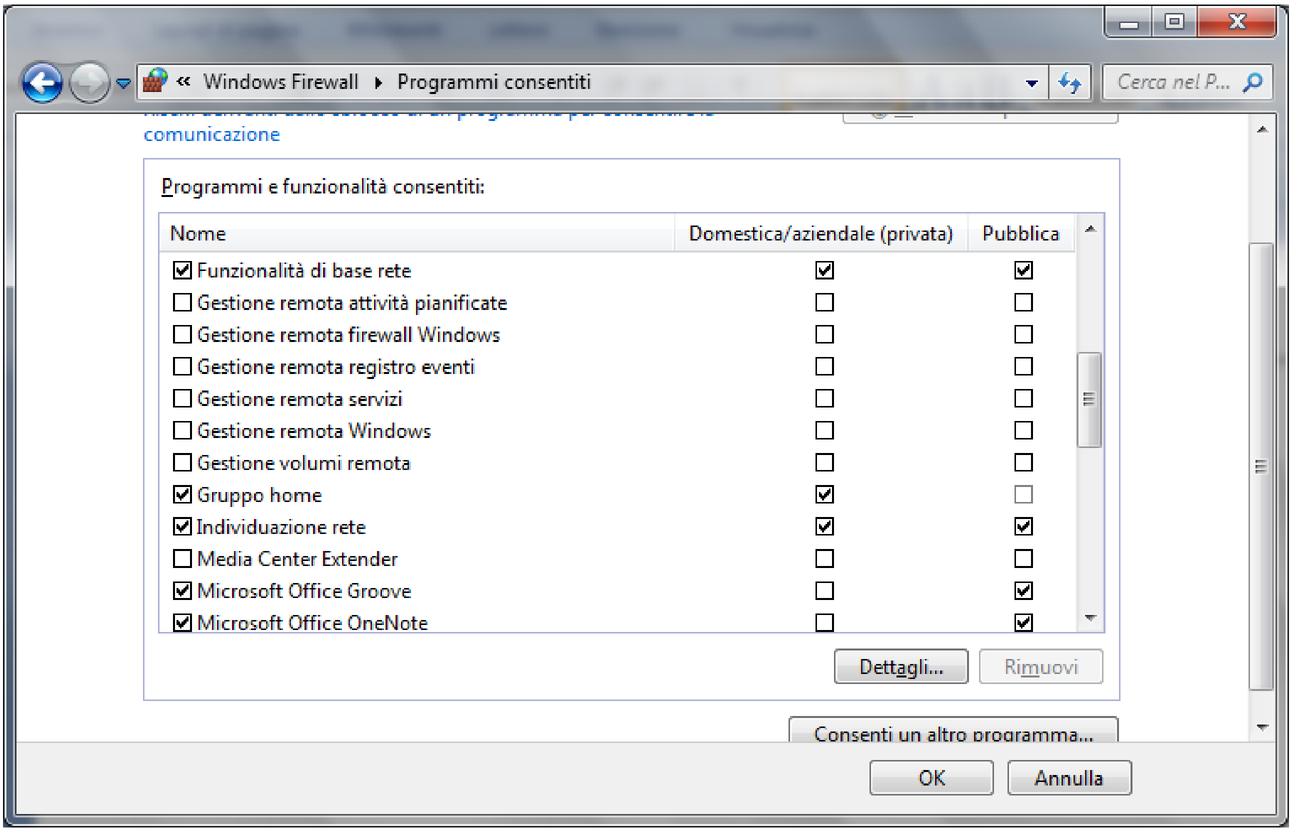


Con due clic sull'icona appare la finestra iniziale del firewall.

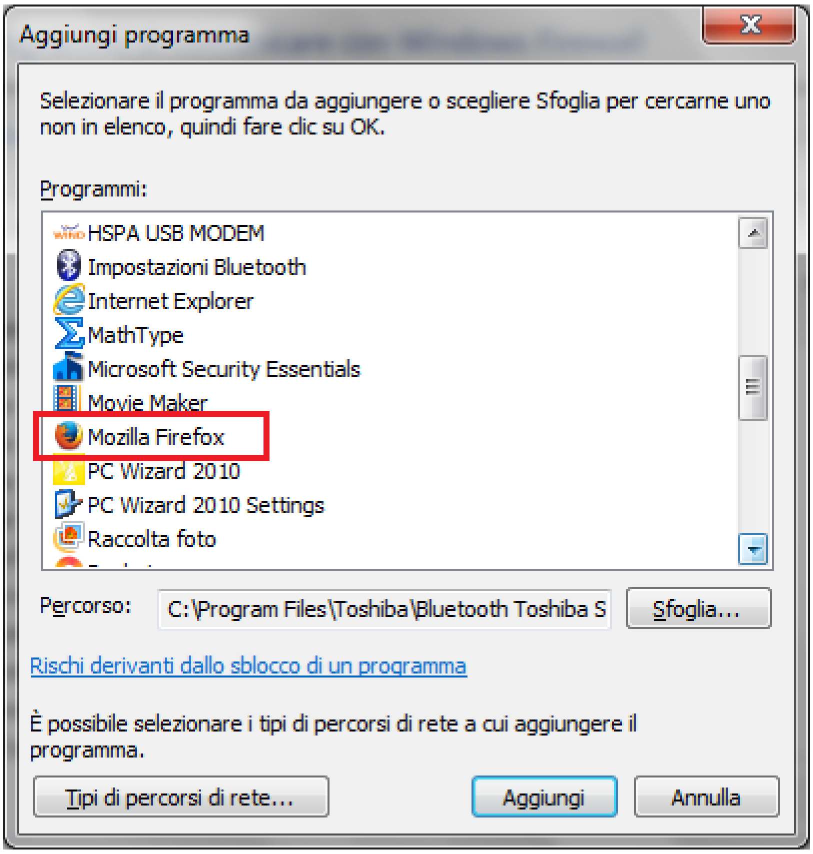


Da questa finestra è possibile Disattivare o attivare il firewall con il comando **Attiva/Disattiva Windows Firewall**.

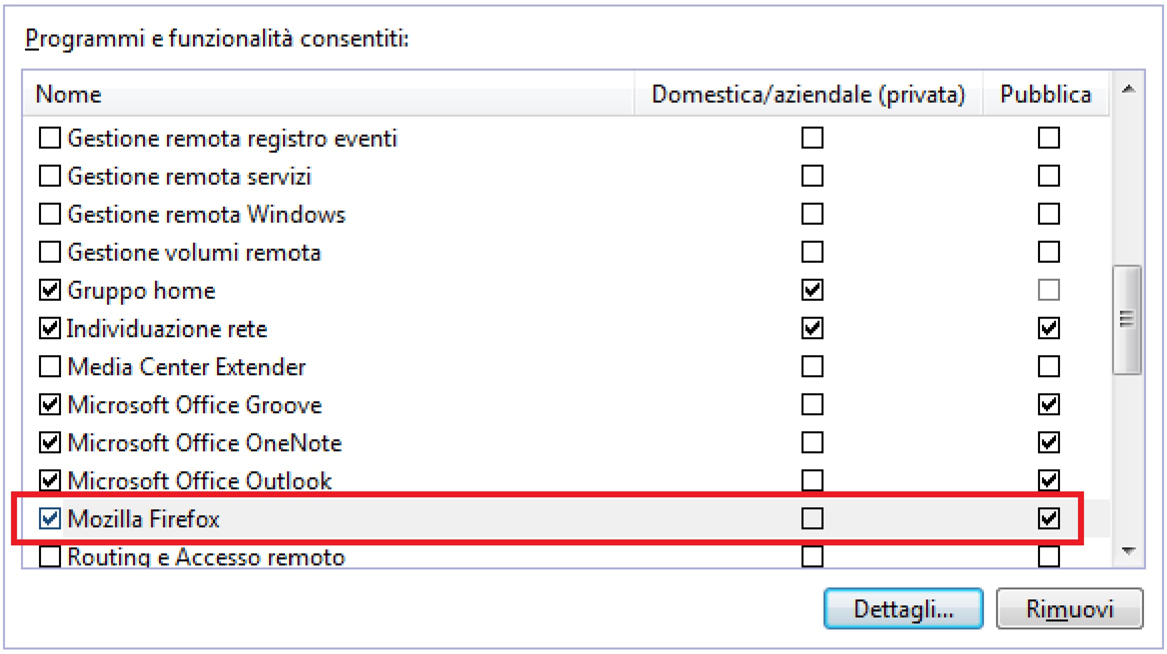
Per aggiungere un programma fare clic su Consenti programma o funzionalità con Windows Firewall.



A questo punto, basta selezionare la casella di controllo accanto al programma che si desidera abilitare. Se il programma non appare nell'elenco, come nel nostro caso, si può aggiungerlo con il comando **Consenti un altro programma**. Verrà visualizzata la finestra **Aggiungi programma**.



Se non appare il programma nella lista, con un clic sul pulsante **Sfoglia** si può navigare fino alla cartella di installazione di Firefox (cioè C:\Program Files\Mozilla Firefox\) e scegliere firefox.exe.
A questo punto, fare clic sul pulsante **Aggiungi** e sul pulsante **OK** per chiudere la finestra dei programmi consentiti.

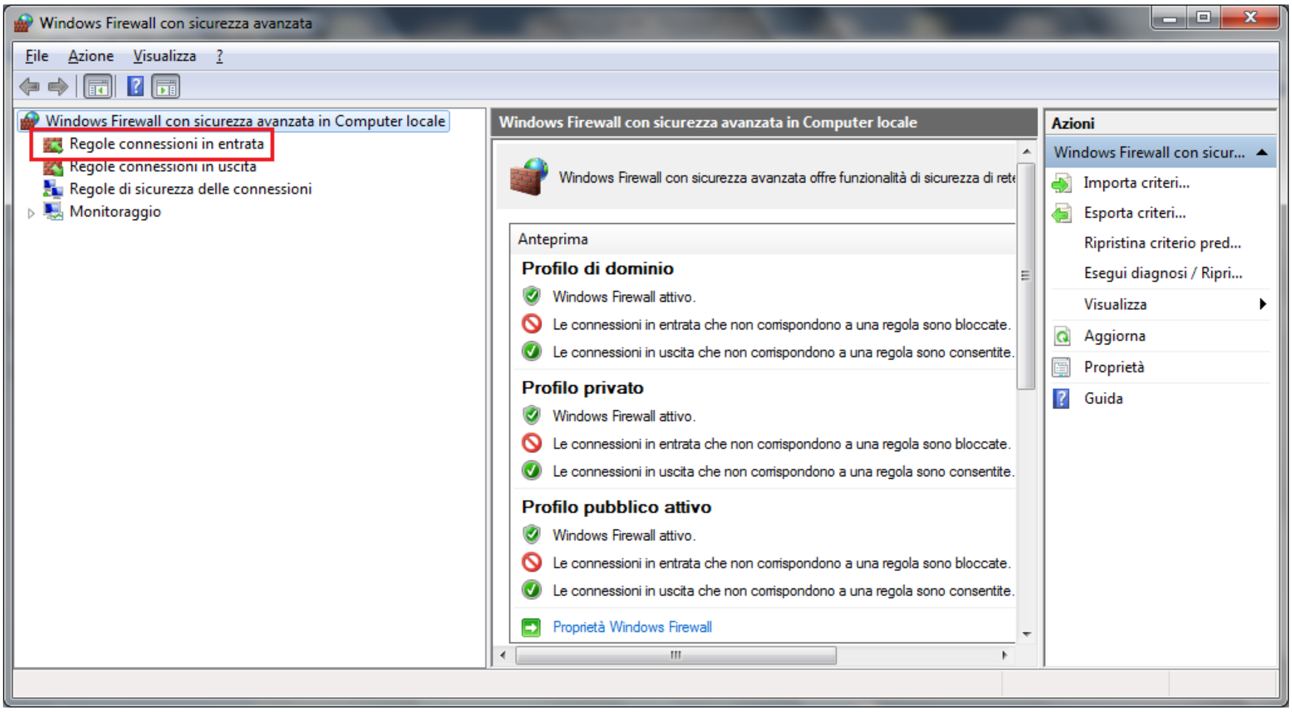


Ad ogni programma consentito si possono associare due tipologie di rete:

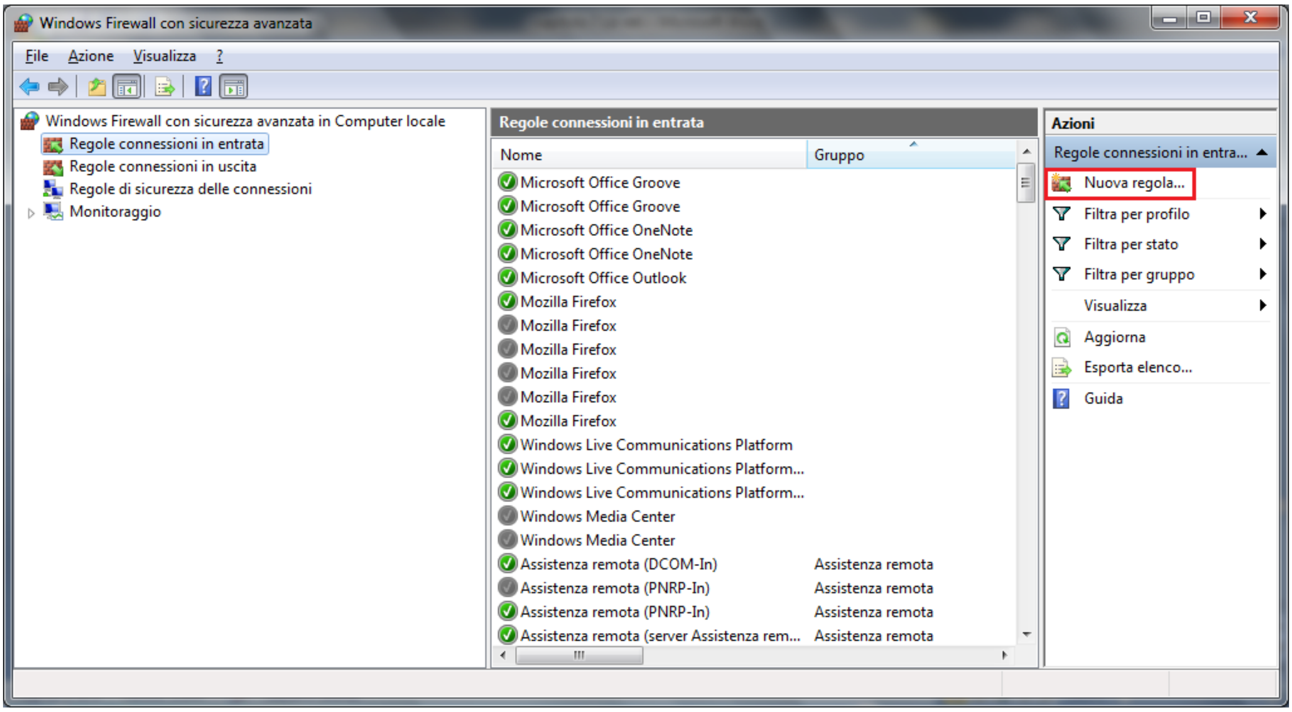
Domestica/aziendale (privata): sono le reti interne al proprio domicilio o azienda. In generale le reti dove i computer collegati si considerano attendibili e “sicuri”.
Pubblica: sono reti in luoghi pubblici, quali Internet café o aeroporti. Se questo percorso è disabilitato si impedisce agli altri computer nelle vicinanze la visualizzazione del computer in uso, in modo da proteggerlo da qualsiasi software dannoso proveniente da internet.

Configurare il firewall di Windows: aggiungere o togliere regole

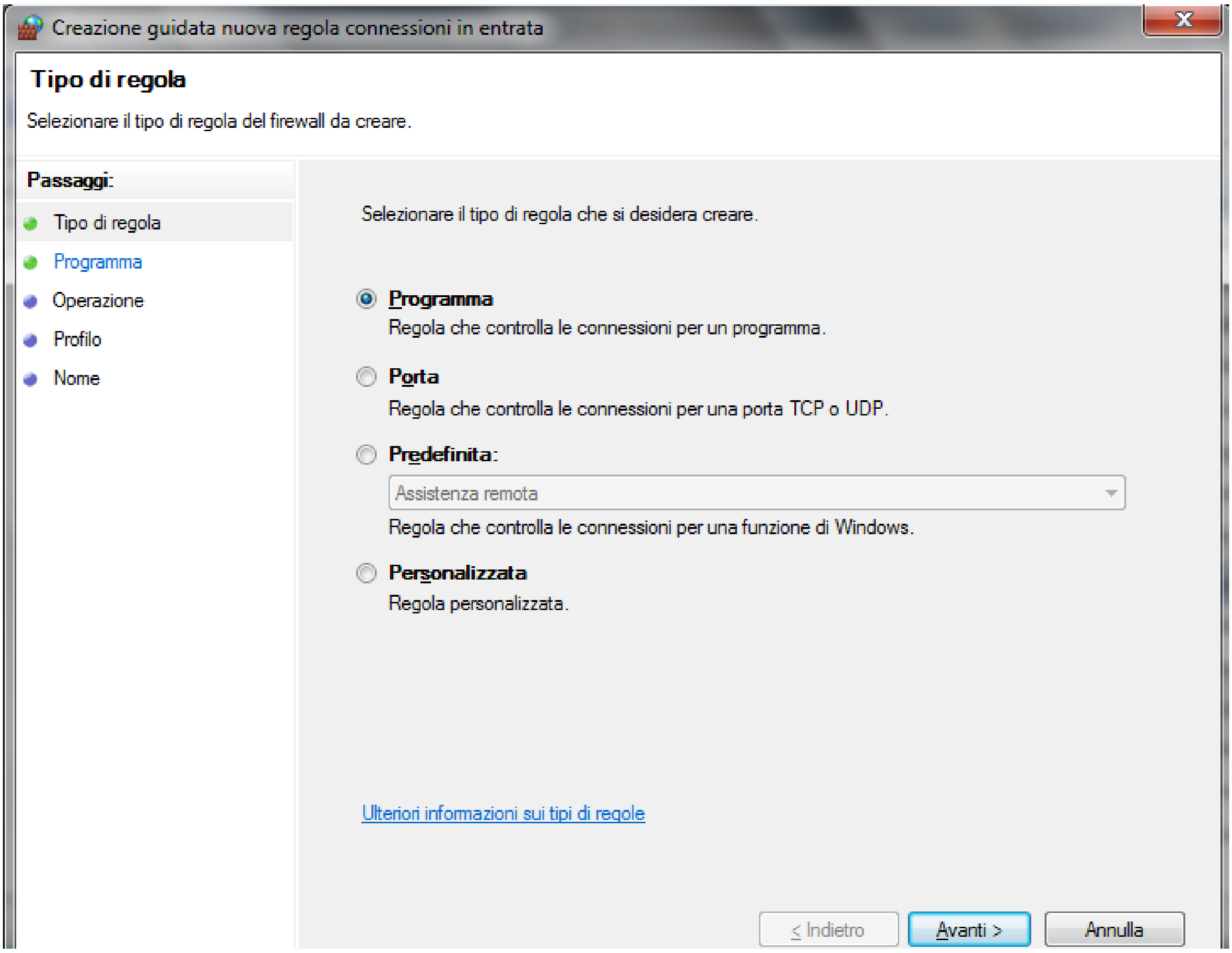
Aggiungendo un programma si apre un ulteriore accesso attraverso il firewall solo quando il programma è in esecuzione.
Ci possono essere dei casi in cui si preferisce aprire una **porta** di comunicazione, ad esempio se si desidera rendere disponibile un programma su un computer ad altri utenti tramite internet. Una porta è un numero che va da 0 a 65535 e serve ai computer per capire a che programma devono essere deviati i dati che arrivano. Possiamo pensare che se il computer fosse un condominio, il numero di IP (numero che identifica il computer nella rete) sarebbe l’indirizzo dell’edificio. La porta possiamo immaginarla come uno degli appartamenti interni al condominio, in cui ogni appartamento è un programma che vuole comunicare con internet.
Nel caso precedente abbiamo visto come consentire (o non consentire) ad un programma di ricevere o inviare dati attraverso il firewall. In questo caso siamo ad un livello più dettagliato: si specifica *attraverso quale porta* un programma può ricevere o inviare i dati o, viceversa, quale porta non deve usare per queste operazioni.
Di norma, un firewall blocca preventivamente qualsiasi tentativo proveniente dalla rete di accedere alle applicazioni installate sul sistema o alle funzionalità del sistema operativo. Ma, in talune circostanze, consentire l'accesso da remoto a certi programmi in esecuzione sul PC può essere una azione desiderata. Facciamo il caso che ci sia un programma che debba condividere file e cartelle con alcuni utenti remoti, cioè si comporti comporta come una sorta di server web. In questo caso si deve creare una specifica regola in entrata. Oppure se si desidera partecipare con gli amici a un gioco di gruppo su internet, potrebbe essere necessario aprire una specifica porta per il gioco in modo che il firewall consenta alle informazioni relative al gioco di raggiungere il computer. Altri esempi possono essere software per il peer-to-peer, le chat, la videoconferenza, ecc.
In questo caso la porta rimarrà sempre aperta: bisogna ricordarsi di chiuderla quando non sarà più necessario tenerla aperta.
Dalla finestra iniziale di Microsoft Firewall scegliere **Impostazioni avanzate**. Appare la finestra **Windows Firewall con sicurezza avanzata**.



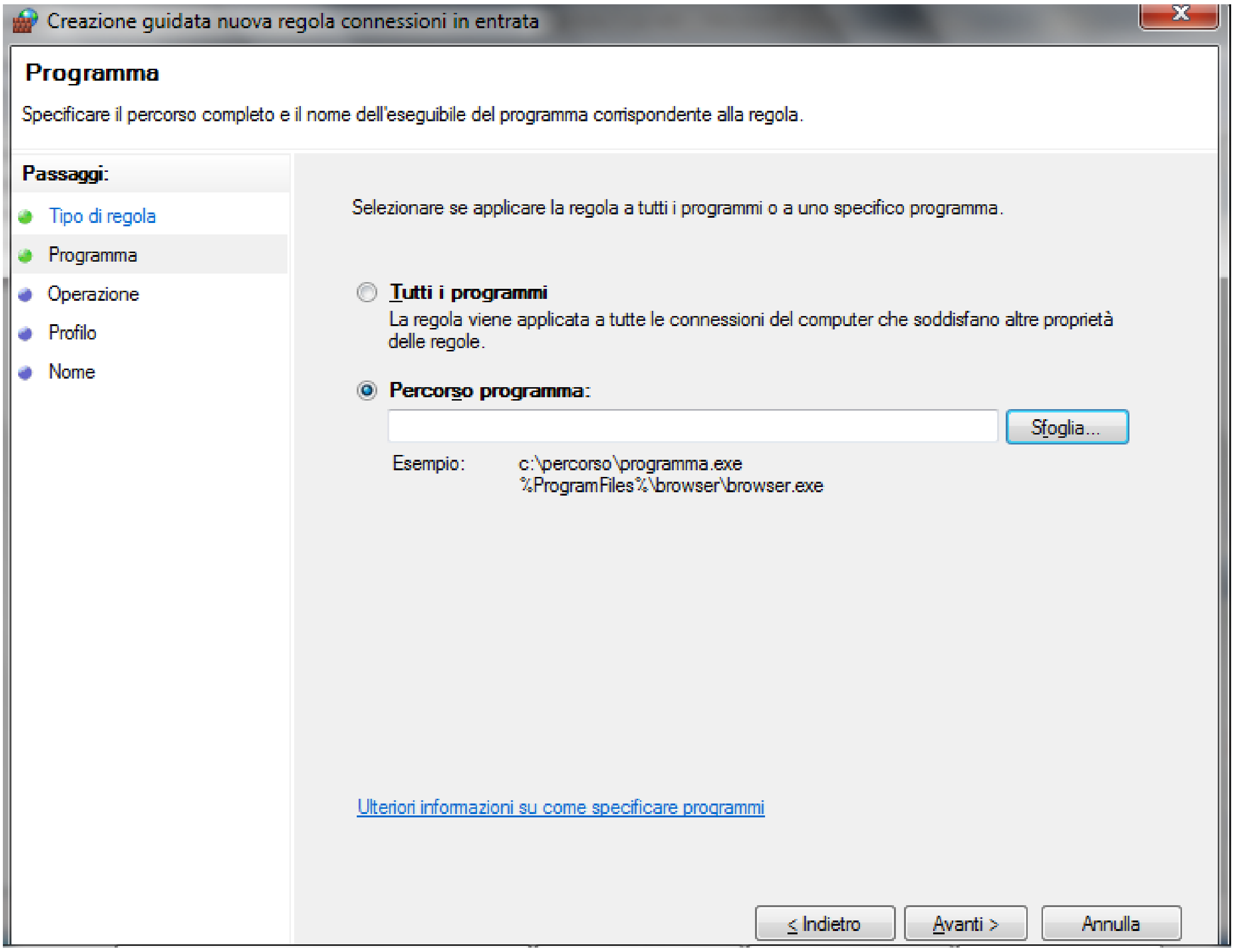
I comandi presenti in questa finestra sono molto specifici ed è preferibile che siano utilizzati solo da utenti esperti. Ci limitiamo a trattare solo un esempio di aggiunta di una regola di connessione in entrata, che poi elimineremo.
Nella colonna di sinistra scegliere **Regole connessioni in entrata**.



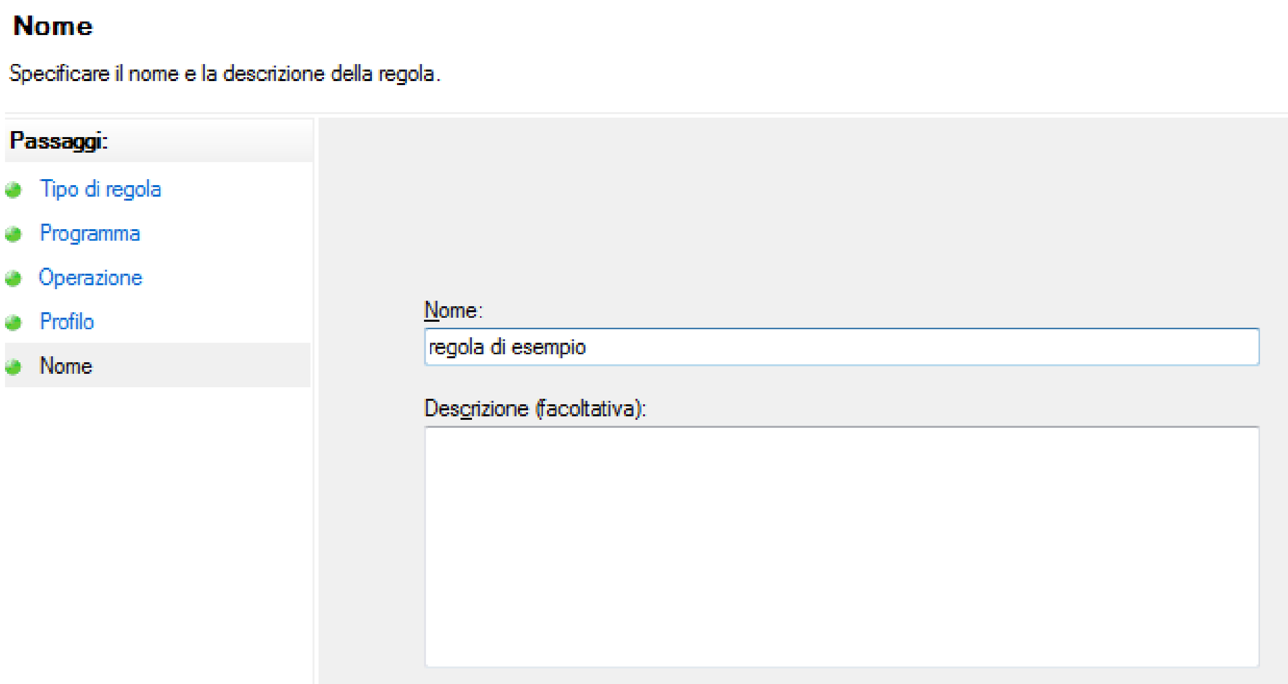
Appare l'elenco delle regole abilitate (icona verde) e disabilitate (icona grigia). Fare clic su **Nuova regola** (riquadro di destra) per iniziare la procedura guidata di creazione di una regola.



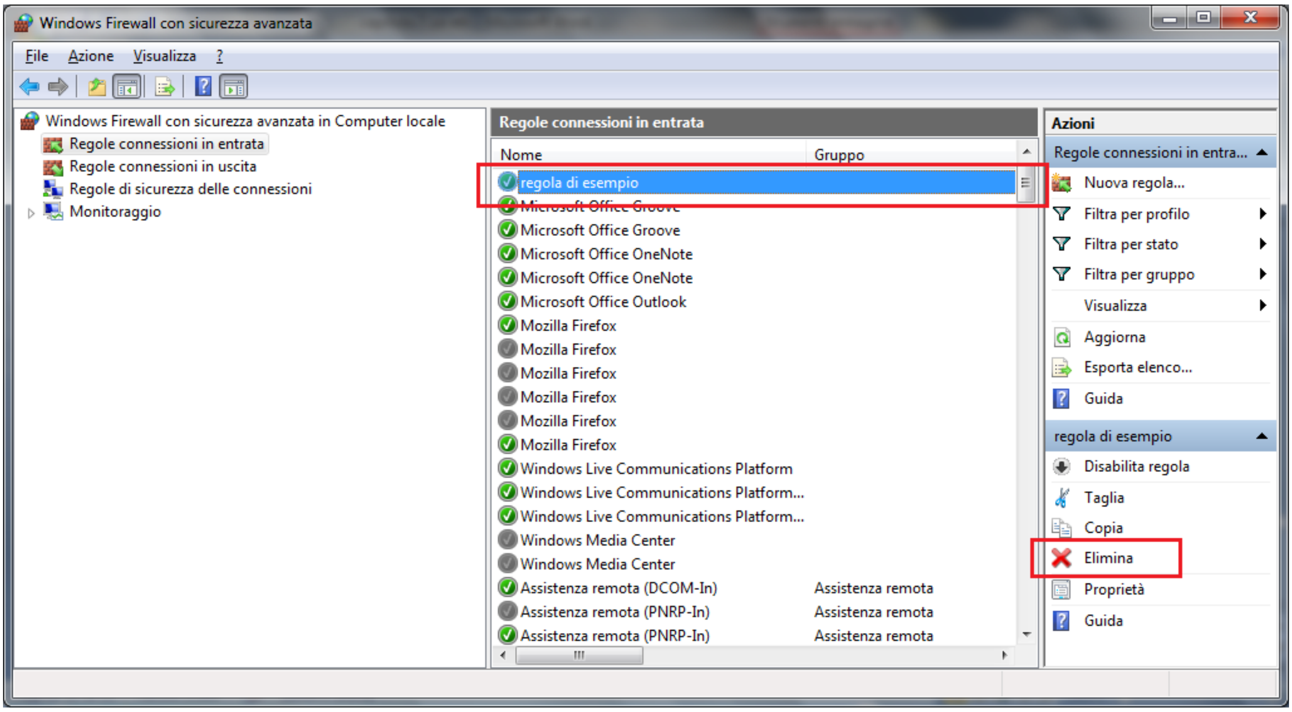
Windows Firewall con sicurezza avanzata offre quattro tipi di base di regole firewall. Utilizzando uno di questi tipi di regole firewall, è possibile creare eccezioni per consentire o negare in modo esplicito una connessione attraverso Windows Firewall.
Vediamo solo il caso di regola di **Programma** per autorizzare una connessione a seconda del programma che tenta di stabilirla.
Fare clic su **Avanti** per specificare il percorso del file del programma.



Scegliere un programma qualunque. Nel nostro esempio abbiamo scelto CCleaner. I passaggi successivi riguardano la scelta della porta per la connessione e del dominio e sono troppo tecnici: fare ripetutamente clic su **Avanti**, fino ad arrivare al nome della regola.



Inserire un nome fittizio e fare clic su **Fine**. La nuova regola appare nell’elenco delle regole.



Cancella la regola dall'elenco con il comando **Elimina**.

Configurare il firewall di Windows: considerazioni conclusive

Quando si aggiunge un programma all'elenco dei programmi consentiti in un firewall o si apre una porta di un firewall, si consente a un programma specifico di inviare o ricevere informazioni nel computer attraverso il firewall. Consentire a un programma di comunicare attraverso un firewall, operazione denominata talvolta **sblocco**, equivale ad aprire una breccia nel firewall.

Ogni volta che si apre una porta o si consente a un programma di comunicare attraverso un firewall, si riduce leggermente la sicurezza del computer. Maggiore è il numero di programmi consentiti o di porte aperte nel firewall, maggiori sono le opportunità per i pirati informatici o per il software dannoso di utilizzare una di tali aperture per diffondere un worm, accedere ai file o utilizzare il computer per diffondere software dannoso ad altri utenti.

È più sicuro, in genere, aggiungere un programma all'elenco dei programmi consentiti anziché aprire una porta. Una porta rimane aperta finché non viene chiusa, indipendentemente dal fatto che venga utilizzata o meno da un programma. Se si aggiunge un programma all'elenco dei programmi consentiti, la "breccia" viene aperta solo quando richiesto per una particolare comunicazione.

Per ridurre i rischi relativi alla sicurezza:

1. Consentire un programma o aprire una porta solo se strettamente necessario e rimuovere programmi dall'elenco dei programmi consentiti oppure chiudere le porte quando queste configurazioni non sono più necessarie. Come regola generale, si concede l'accesso a internet solo ai programmi che conosciuti e solo se la loro richiesta ha un senso. Per esempio, è ovvio che il browser (che sia Internet Explorer, Firefox, Chrome o quant'altro) avrà bisogno di accedere a internet, se vogliamo usarlo: il compito di un browser è appunto quello di navigare nei siti internet, per cui gli dovremo concedere il permesso di collegarsi a internet. Allo stesso modo, se

utilizziamo un programma per scaricare le e-mail sul nostro computer, avrà bisogno del permesso di collegarsi sia in entrata (per ricevere le e-mail), sia in uscita (per spedire le e-mail). Altri programmi, invece, avranno bisogno di poter accedere a internet solo per eventuali aggiornamenti. Se un programma cerca di collegarsi a internet in un momento in cui, apparentemente, non ha alcun bisogno di collegarsi, allora è sempre meglio negargli il permesso.

2. Non consentire mai a un programma sconosciuto di comunicare attraverso il firewall. Infatti, esiste sempre la possibilità che questo programma sia un virus, che abbiamo preso senza accorgercene, oppure che sia un programma infettato da un virus: in questo caso, l'accesso a internet gli servirà per comunicare con il creatore del virus, passargli le nostre informazioni, oppure aprirgli la porta e farlo entrare nel nostro computer.

Per ritornare alla configurazione iniziale fare clic su **Ripristina impostazioni predefinite**.

Domande

1. Una rete estesa a livello geografico si chiama
    a. LAN
    b. LAN WI FI
    c. MAN
    d. WAN
2. Quale affermazione è corretta?
    a. Il nome utente serve ad identificare l'utente, la password ad autenticare
    b. Il nome utente serve ad identificare l'utente, la password ad autenticare
    c. Il nome utente e la password hanno la stessa funzione
    d. Tutte le affermazioni sono errate
3. L'amministratore di sistema:
    a. Deve implementare politiche di accesso alle risorse della rete con l'assegnazione di account
    b. Deve aver cura di conservare l'elenco degli account in un luogo sicuro
    c. Deve richiedere la modifica periodica delle password
    d. Tutte le affermazioni sono corrette
4. Quale delle seguenti affermazioni riguardo a un firewall è errata?
    a. Serve per proteggere contro aggressioni provenienti dall'esterno
    b. Blocca eventuali programmi presenti sul computer che tentano di accedere ad internet senza il controllo dell'utente
    c. Può essere hardware o software
    d. Opera la scansione antimalware
5. Con un firewall è più sicuro, in genere, aggiungere un programma all'elenco dei programmi consentiti o aprire una porta per un programma?
    a. È più sicuro aggiungere un programma all'elenco dei programmi consentiti
    b. È più sicuro aprire una porta per un programma
    c. Non ci sono differenze riguardo la sicurezza
    d. Tutte le affermazioni sono errate
6. È corretto concedere a un browser di comunicare attraverso il firewall?
    a. No, mai
    b. È corretto
    c. Solo se il browser è Microsoft Explorer
    d. Solo se sia ha un firewall hardware
7. cosa significa VPN?
    a. Very Ping Net
    b. Virtual Private Network
    c. Virtual Public Network
    d. Very Private Net
8. Cos'è il WAP?
    a. Protocollo per reti mobili
    b. Protocollo per reti fisse
    c. Protocollo per mail
    d. Protocollo per IM

Capitolo 8

Connessioni e sicurezza delle reti

Tipologie di connessione

Abbiamo visto che una rete è formata da sistemi di elaborazione connessi tra loro al fine di utilizzare nel miglior modo possibile le risorse disponibili e di offrire vari servizi di comunicazione.
Ogni rete di calcolatori necessita di un supporto fisico di collegamento (cavi o similari) per connettere tra loro i dispositivi; il mezzo trasmissivo utilizzato incide notevolmente sulle caratteristiche della rete in termini di prestazioni e di costo. Inoltre, all’interno di una stessa rete.
In generale si possono distinguere due tipologie:

1. connessione tramite cavo;
2. connessione senza fili (*Wireless* o reti *Wi Fi*, Wireless Fidelity)

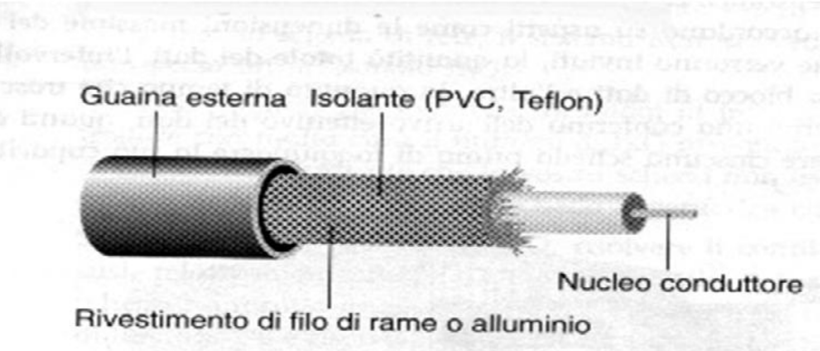
Tutti i mezzi utilizzati hanno la caratteristica di trasportare una qualche forma di energia e quindi sono soggetti a due fenomeni che ne limitano le prestazioni: l'**attenuazione** (dovuta alla resistenza opposta dal mezzo fisico attraversato) ed il **rumore** (la sovrapposizione alle informazioni di segnali provenienti da altri dispositivi vicini).

Connessione tramite cavo

I mezzi trasmissivi tramite cavo possono essere di tipo **elettrico**. Viene sfruttata la capacità dei metalli di condurre energia elettrica. I più comuni sono:
doppino telefonico: è formato da una coppia di fili di rame: permette trasmissioni di dati fino alla velocità di 9600 bps (bit per secondo).Di semplice uso (vengono usati i cavi già posati che consentono le conversazioni telefoniche) ed economico, è il mezzo trasmissivo attualmente più utilizzato sia per reti locali che per alcuni tratti delle reti più grandi.



Cavo coassiale: è formato da un conduttore di rame posto al centro del cavo all’interno di un rivestimento isolante e di uno schermo costituito da fili metallici intrecciati per garantire il massimo isolamento. È particolarmente insensibile alle interferenze elettromagnetiche e consente trasmissioni fino alla velocità di 10 Mbps.



Cavo coassiale.

Altri mezzi trasmissivi sono i **mezzi ottici** che utilizzano la luce per trasferire le informazioni, In particolare le **fibre ottiche.** il supporto fisico dove viaggia la luce è vetro filato in diametri molto piccoli e ricoperto di materiale opaco; con l'attuale tecnologia è possibile ottenere fili di vetro del diametro di poche decine di micron (millesimo di millimetro) robusti e flessibili, di una purezza tale da consentire trasmissioni a centinaia di chilometri alla velocità di 10^9 bps. Grazie al fatto che il segnale è portato da impulsi di luce, le fibre ottiche sono immuni dai disturbi elettromagnetici; inoltre le ridotte dimensioni permettono di inserire in un unico cavo centinaia di fibre. Sono già utilizzate e potrebbero essere il mezzo del futuro dopo l'abbattimento dei loro alti costi (difetto principale delle fibre ottiche).



Connessione senza fili

Le reti senza fili o reti wireless sono prive di cablaggi. I nodi comunicano fra di loro attraverso raggi infrarossi (più raramente) o **onde radio**, dove si sfrutta la possibilità di trasferire variazioni di corrente elettrica a distanza tramite onde elettromagnetiche.

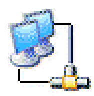


Le connessioni wireless sono quelle che permettono la comunicazione tra i cellulari. Attraverso ponti radio o satellitari le onde elettromagnetiche sono inviate da un trasmettitore e, viaggiando ad una velocità prossima a quella della luce, raggiungono l'antenna del ricevente (eventualmente utilizzando uno o più satelliti). Sono usati per collegamenti a grandi distanze visto che, quasi indipendentemente dalle posizioni del trasmettitore e del ricevitore, il ritardo nelle comunicazioni è dell'ordine delle centinaia di millisecondi. L'ostacolo maggiore alla diffusione di tali tecniche è l'elevato costo.
Questo tipo di rete si rivela utile quando non sia possibile posare cavi (ad esempio in edifici storici), oppure nel caso in cui si voglia consentire il funzionamento della rete con l'elaboratore e l'utente in movimento.
In questi anni si sono diffusi gli **hotspot WiFi**: sono dei punti di accesso ad internet, con tecnologia wireless, aperti al pubblico.
Un HotSpot WiFi è quindi un'area nella quale è possibile accedere ad internet tramite il proprio dispositivo WiFi. Tale area deve essere creata da dispositivi programmati appositamente per offrire un servizio sicuro e controllato. Solitamente gli HotSpot WiFi utilizzano delle antenne per creare reti accessibili senza l'ausilio di cablature. Le figure sottostanti rappresentano i tipici avvisi per zone WiFi.



Vantaggi e svantaggi delle due tipologie di connessione

Una rete cablata con mezzi trasmissivi fisici, come i cavi, offre una maggior *sicurezza* dato che la connessione fisica tra i dispositivi è visibile. Si vedono, o si conoscono, i computer connessi tra loro. In figura, l'icona di una rete cablata, nel sistema operativo Windows.



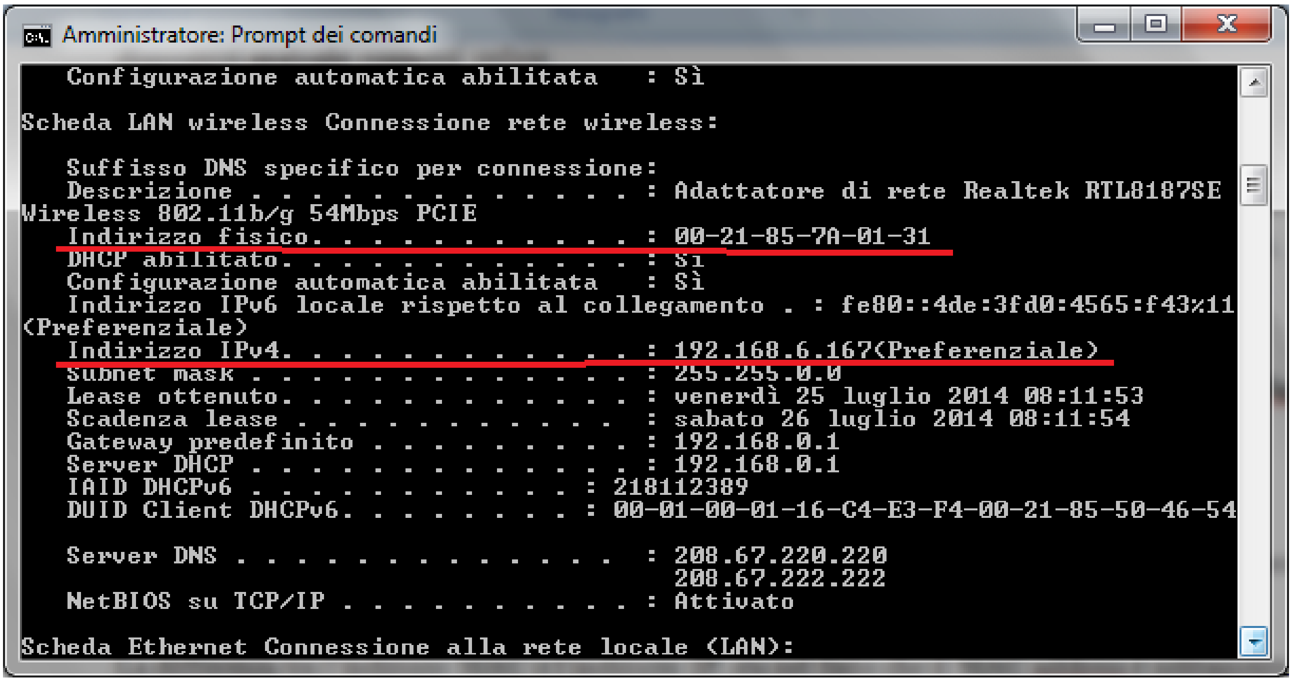
I vantaggi di una rete senza fili sono l'*economicità* e la *praticità*. Non si deve posare un cavo di collegamento agli altri dispositivi. Per lo stesso motivo una rete wireless è più facilmente *espandibile*. Chiaramente, se non è protetta da un efficiente sistema di autenticazione, è più *vulnerabile* ad accessi non autorizzati. I rischi, già visti in precedenza, sono:

1. infezioni da virus o altro malware;
2. furto di dati;
3. violazione della privacy, ecc.

Sicurezza per reti wireless

Abbiamo visto che una rete cablata richiede un collegamento fisico agli elementi della rete. Per questo motivo, è quasi impossibile collegare un dispositivo senza autorizzazione da parte dell'amministratore di rete.
Invece, in una rete senza fili, non fornita di adeguata protezione, ci si può facilmente agganciare con un dispositivo mobile, anche posto all'esterno dell'edificio fin dove arriva il segnale wireless. È possibile navigare "a scrocco" dell'inconsapevole proprietario del segnale, ma questo non è un grande problema.
Il problema è che qualcuno male intenzionato può entrare nella nostra rete WiFi e intercettare il flusso dati o entrare in qualche cartella o disco condiviso carpendo le nostre informazioni.
Più si diffondono le reti WiFi più aumenta l'esigenza di sicurezza: si sono così messi appunto dei sistemi di autenticazione e di crittografia appositi per le reti Wireless. Attualmente la maggior parte dei router e adattatori wireless per pc supportano i più diffusi sistemi di autenticazione wireless.
In ogni rete Wireless, il router wireless oltre al segnale radio trasmette anche un segnale identificativo della rete, chiamato *SSID* (Service Set Iidentifier), che non è altro che il nome della rete a cui i dispositivi dotati di un adattatore wireless possono connettersi. Se non ci sono meccanismi di protezione, si ha una autenticazione *Open* o *Aperta*. Appena il router Wireless viene accesso, emette il segnale ed il SSID, e chi rientra nell'hotSpot WiFi può connettersi liberamente alla rete: ecco perché si dice aperta. Il livello di protezione offerto da questo livello di autenticazione è praticamente nullo, chiunque può entrare, i dati sono scambiati in chiaro, ed in più sono a rischio anche le risorse di rete condivise.
Proprio per sopperire alla mancanza di protezione, se si dispone di una rete wireless, è consigliabile configurare una **chiave di sicurezza di rete**, che consente di attivare la crittografia.
La chiave di sicurezza è un codice che impedisce la connessione alla rete a chi non la possiede e permette di crittografare i dati inviati da un computer di una rete ad un altro in modo che sia possibili leggerli solo se si è in possesso della chiave.
I metodi di Autenticazione di una rete Wireless sono:
Autenticazione con chiave WEP: WEP significa **Wired Equivalent Privacy** (in italiano privacy equivalente alla rete cablata). Nasce nel 1999 e fa parte dello standard per le comunicazioni *WiFi*, universalmente riconosciuto e montato su praticamente tutti i dispositivi.
Il suo funzionamento si basa su una password di protezione per accedere alla rete, la **chiave WEP**, che è la stessa tra tutti gli utenti che accedono alla rete. La chiave WEP è una password alfanumerica, impostata sul router, è può essere di diversa lunghezza, quali: 64,

128 e 256bit, più lunga sarà la chiave maggiore sarà il livello di crittografia dei dati e conseguentemente la protezione. D'altro canto però una cifratura maggiore comporta un calo della velocità e delle prestazioni, a causa del maggiore onere di calcolo per crittografare dati con una chiave così lunga.
Il sistema di autenticazione wireless con chiave WEP, come tipo di crittografia, è stata superata ed ora è considerata come la minima protezione necessaria per la sicurezza di una rete senza fili. Il suo uso è in declino, soppiantato dal sistema **WPA**.
Autenticazione con chiave WPA: l'autenticazione con chiave WPA (WiFi Protected Access) è simile alla chiave WEP, ma ha un livello di protezione maggiore, poiché usa un algoritmo per l'offuscamento e la crittografia dei dati differente dal primo. Il WPA, sua forma certificata e più attuale **WPA 2**, è il principale sistema di sicurezza nelle rete senza fili. Solo recentemente alcuni hacker sono riusciti a violarlo. È stato proposto un nuovo standard evoluto chiamato **WPA-AES** che è tuttora lo standard più avanzato di sicurezza WLAN. L'uso dell'autenticazione con chiave WPA si sta allargando, e sicuramente andrà a sostituire quello con chiave WEP, bisogna inoltre aggiungere che i due sistemi non sono compatibili reciprocamente.
Autenticazione Condivisa con chiave WPA-PSK: l'acronimo WPA-PSK (**WiFi Protected Access - Pre Shared Key**) indica che viene usata una chiave condivisa di autenticazione, come in WEP, basato su un metodo di cifratura però simile a WPA. È una di via di mezzo tra la chiave WEP e quella WPA. Offre maggiore protezione di WEP ma inferiore a WPA. Rispetto a quest'ultimo gode del vantaggio di avere un hardware più semplice e dai costi più ridotti.
Un ulteriore codice di sicurezza è il **MAC**. MAC è un acronimo che sta per **Media Access Control**. Tutti i dispositivi di rete, sia quelli diventati obsoleti e finiti in discarica, sia quelli tutt'ora in uso (e addirittura anche quelli progettati ma non ancora prodotti) hanno un codice univoco, il codice MAC, che permette di identificare univocamente il dispositivo dotato di connettività Internet (un router Wi-Fi, la scheda ethernet di un computer, una stampante di rete, ecc.) tra i milioni di dispositivi analoghi connessi online.
Quindi, la funzione primaria di un indirizzo MAC è quella di identificare univocamente un dispositivo di rete tra i miliardi presenti online. Questa caratteristica può essere utilizzata per "mettere in sicurezza" la rete locale (LAN). L'amministratore di rete può concedere l'accesso alla rete solo a dispositivi il cui MAC address è conosciuto e di cui ci si può fidare. In questo modo, almeno in teoria, si crea un muro a difesa della propria rete. Purtroppo esistono dei software in grado di modificare il Mac address della scheda di rete di un dispositivo.
Per trovare l'indirizzo MAC del computer in uso, aprire il prompt dei comandi, digitare **ipconfig/all** e premere INVIO.



```
Amministratore: Prompt dei comandi
   Configurazione automatica abilitata   : Sì

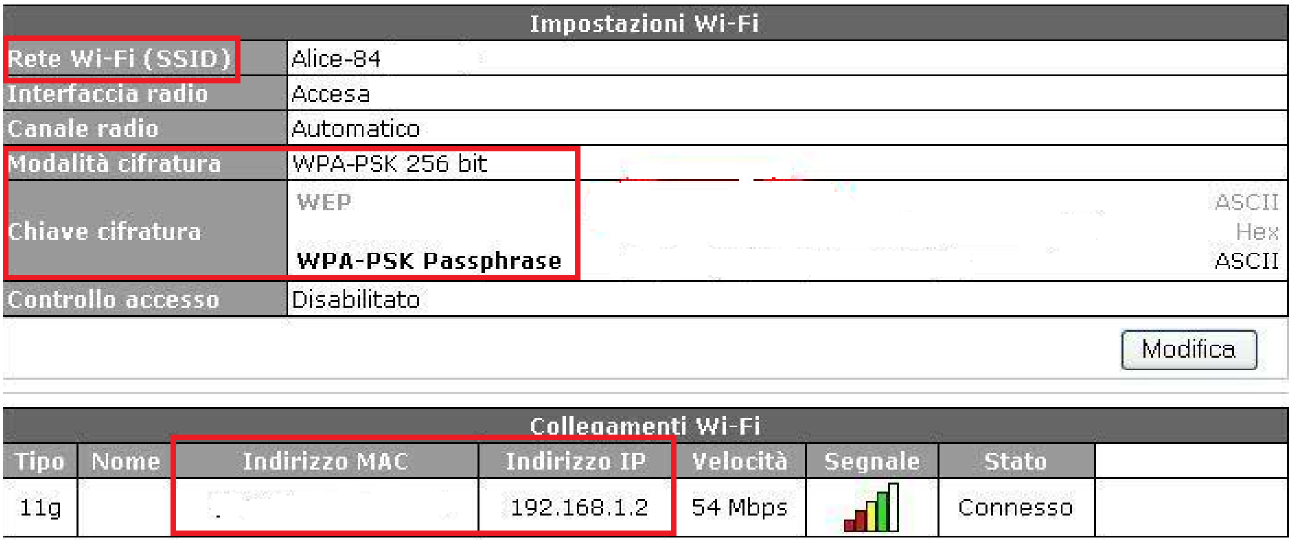
Scheda LAN wireless Connessione rete wireless:

   Suffisso DNS specifico per connessione:
   Descrizione . . . . . . . . . . . . . : Adattatore di rete Realtek RTL8187SE
Wireless 802.11b/g 54Mbps PCIE
   Indirizzo fisico. . . . . . . . . . . : 00-21-85-7A-01-31
   DHCP abilitato. . . . . . . . . . . . : Sì
   Configurazione automatica abilitata   : Sì
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::4de:3fd0:4565:f43%11
(Preferenziale)
   Indirizzo IPv4. . . . . . . . . . . . : 192.168.6.167(Preferenziale)
   Subnet mask . . . . . . . . . . . . . : 255.255.0.0
   Lease ottenuto. . . . . . . . . . . . : venerdì 25 luglio 2014 08:11:53
   Scadenza lease . . . . . . . . . . .  : sabato 26 luglio 2014 08:11:54
   Gateway predefinito . . . . . . . . . : 192.168.0.1
   Server DHCP . . . . . . . . . . . . . : 192.168.0.1
   IAID DHCPv6 . . . . . . . . . . . : 218112389
   DUID Client DHCPv6. . . . . . . . : 00-01-00-01-16-C4-E3-F4-00-21-85-50-46-54

   Server DNS . . . . . . . . . . . . .  : 208.67.220.220
                                           208.67.222.222
   NetBIOS su TCP/IP . . . . . . . . . . : Attivato

Scheda Ethernet Connessione alla rete locale (LAN):
```

Se nel computer è installata più di una scheda di rete, l'indirizzo fisico di ogni scheda verrà elencato separatamente.
La differenza tra l'indirizzo MAC e l'indirizzo IP, sta nel fatto che il MAC address è solitamente definito a livello hardware, assegnato dal produttore e non cambia mai nel tempo (a meno di interventi dell'amministratore di rete); l'indirizzo IP viene definito a livello software e può anche cambiare ad ogni nuova connessione alla rete.
Tutti i termini descritti si possono incontrare quando si imposta una nuova connessione WiFi, come in figura.



Impostazioni Wi-Fi	
Rete Wi-Fi (SSID)	Alice-84
Interfaccia radio	Accesa
Canale radio	Automatico
Modalità cifratura	WPA-PSK 256 bit
Chiave cifratura	WEP ASCII Hex WPA-PSK Passphrase ASCII
Controllo accesso	Disabilitato

Modifica

Collegamenti Wi-Fi						
Tipo	Nome	Indirizzo MAC	Indirizzo IP	Velocità	Segnale	Stato
11g			192.168.1.2	54 Mbps		Connesso

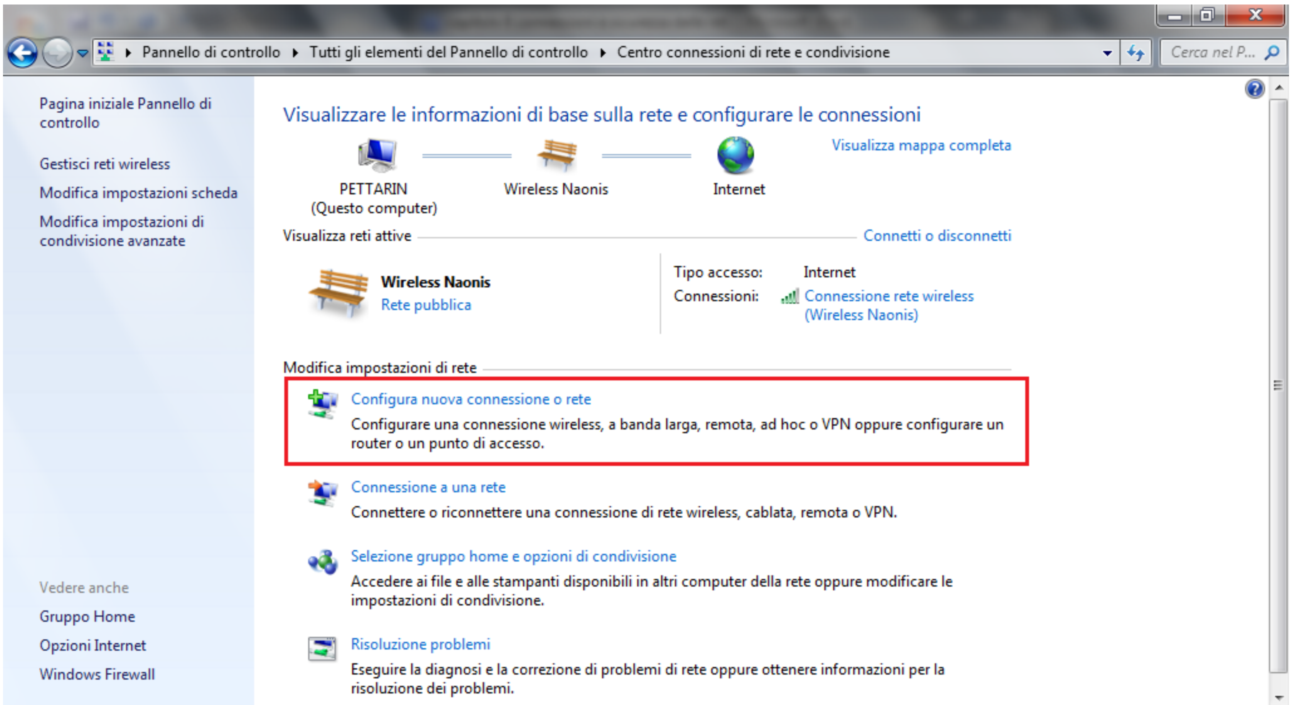
Quando si aggiunge un nuovo dispositivo di rete, bisogna ovviamente essere certi che il suo indirizzo IP di default non sia già in uso sulla stessa rete. Molti dispositivi di rete, come i modem router ADSL, utilizzano 192.168.1.1 come indirizzo IP di default. È un indirizzo IP meno "sicuro" di altri.

Configurare una rete computer-to-computer (ad hoc)

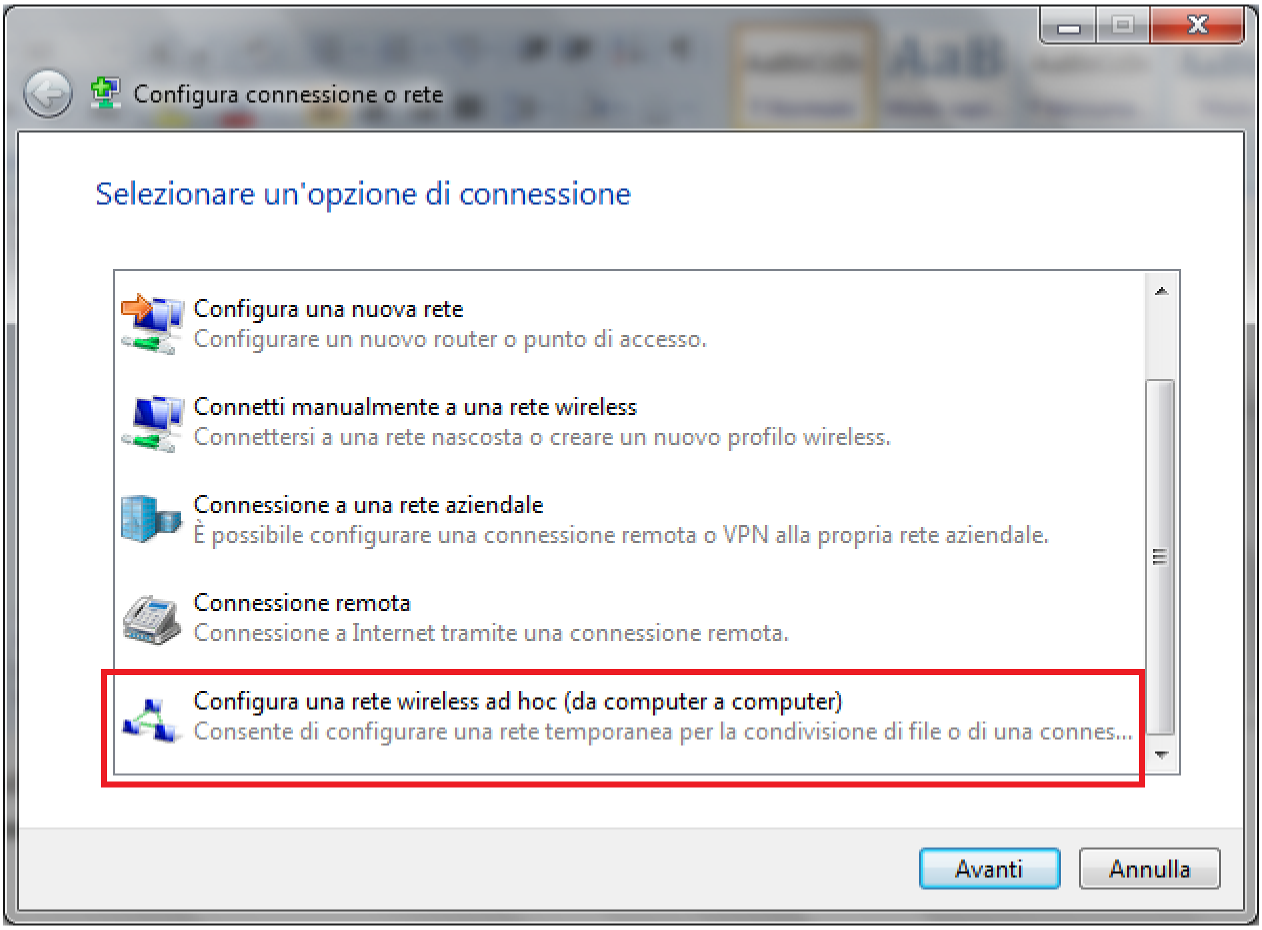
Per rivedere i concetti illustrati nei paragrafi precedenti proviamo a configurare una rete **computer-to-computer (ad hoc)** con Windows 7.

Una rete ad hoc è una connessione temporanea tra computer e dispositivi utilizzati per uno scopo specifico, ad esempio per la condivisione di file o presentazioni durante una riunione o l'esecuzione di giochi per computer con più giocatori. È inoltre possibile condividere temporaneamente una connessione internet con altri utenti nella rete ad hoc, in modo che tali utenti non debbano configurare altre connessioni internet. Poiché le reti ad hoc possono essere solo wireless, è necessario che nel computer in uso sia installata una scheda di rete wireless per configurare o accedere a una rete ad hoc. Inoltre i computer devono trovarsi a non più di 10 metri di distanza.

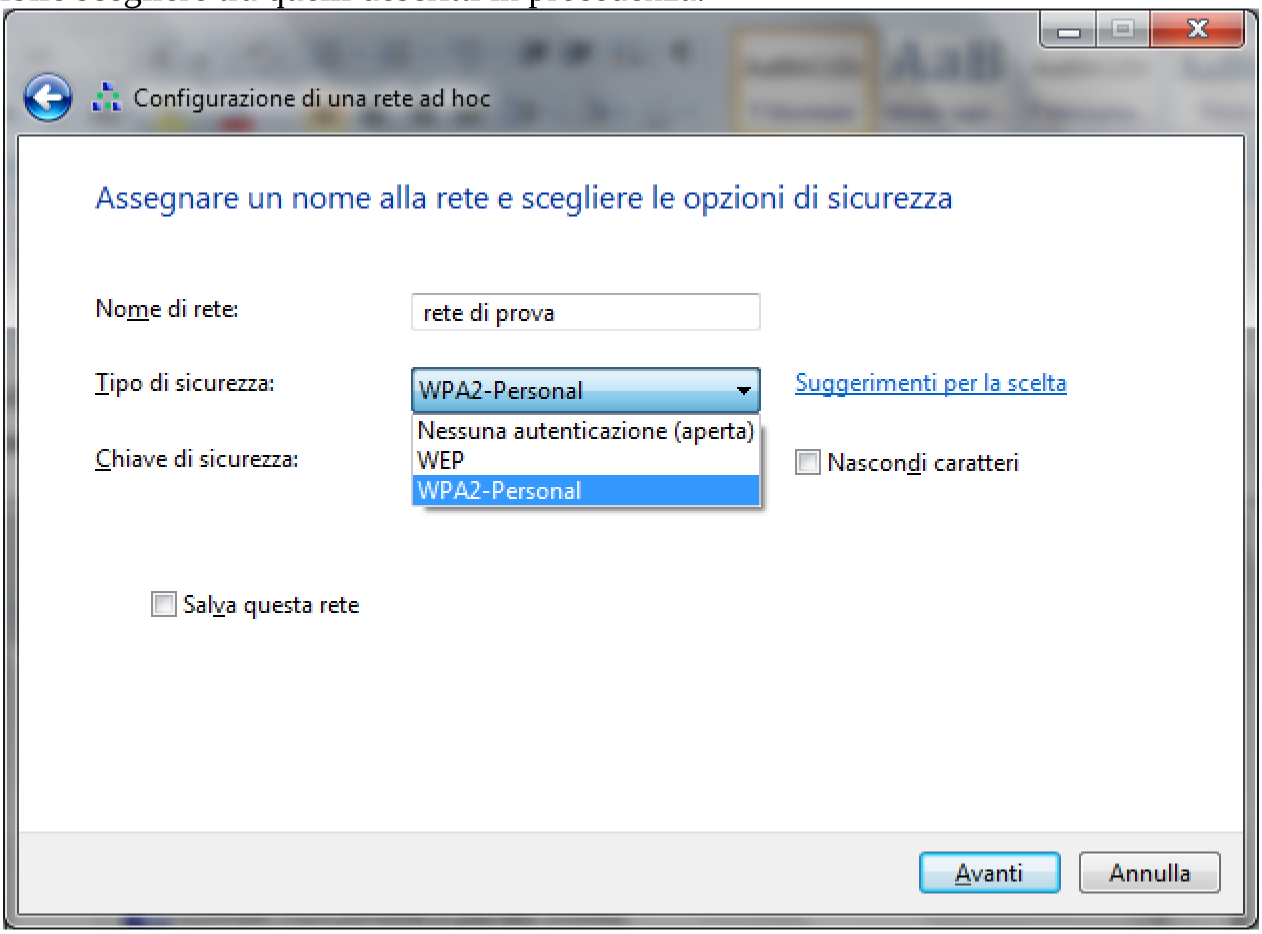
Per configurare questo tipo di rete si deve aprire il **Centro connessioni di rete e condivisione** (dal Pannello di controllo) e fare clic su **Configura nuova connessione o rete**.



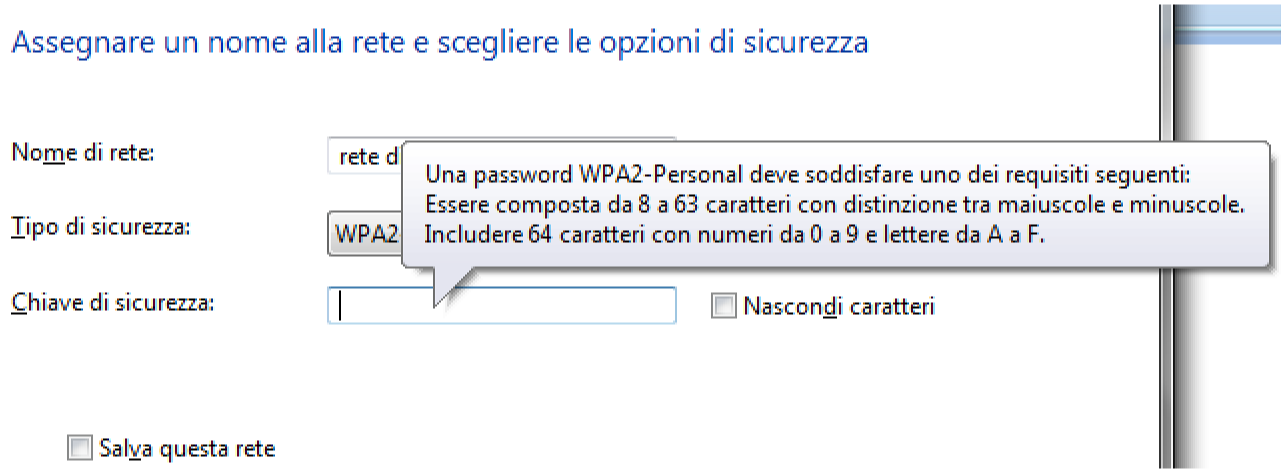
Nell'elenco delle opzioni di connessione, scegliere **Configura una rete wireless ad hoc (da computer a computer) e** fare clic su **Avanti** (per due volte).



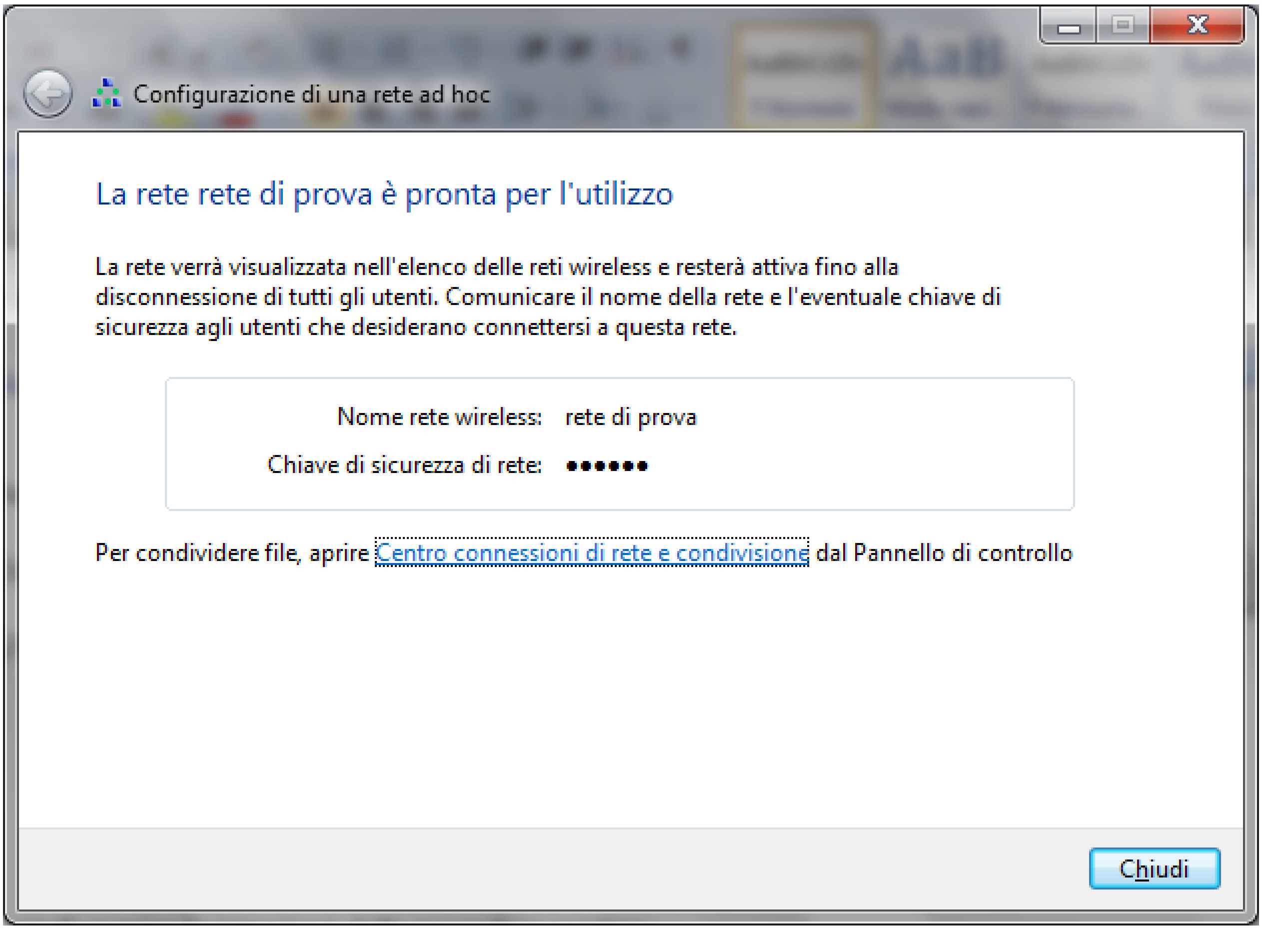
Nella finestra successiva si assegna il **Nome della rete** (SSID) e il **Tipo di sicurezza**: è possibile scegliere tra quelli descritti in precedenza.



In particolare si può inserire una **Chiave di sicurezza**, una password per l'accesso a questa rete.



La procedura di creazione della rete è terminata. Come è descritto in figura, la rete è presente nell'elenco delle reti wireless disponibili. La rete sparirà automaticamente, quanto tutti gli utenti si saranno disconessi.



Conclusioni

Se si ha a disposizione una rete wireless i suggerimenti per un utilizzo, nella massima sicurezza possibile, sono:

utilizzare la crittografia WPA2, se possibile. Non è consigliabile utilizzare WEP per la sicurezza della rete. WPA e WPA2 sono metodi più sicuri;

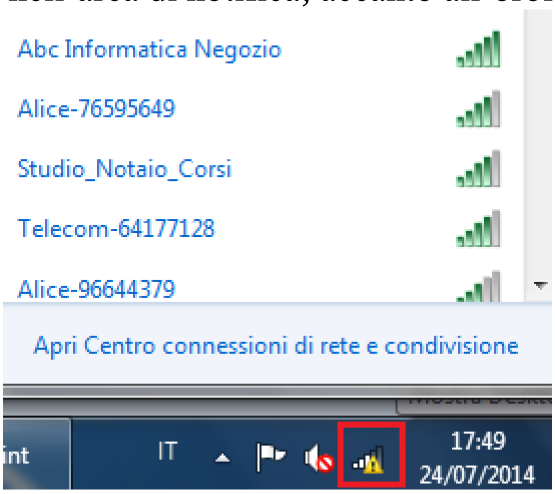
cambiare il SSID predefinito: abbiamo visto come i router e i punti di accesso utilizzano un nome di rete wireless noto come identificatore del set di servizi (SSID). La maggior parte dei produttori utilizza lo stesso SSID per tutti i router e punti di accesso. È pertanto consigliabile modificare il SSID predefinito per evitare che la rete wireless in uso si sovrapponga ad altre reti wireless che potrebbero utilizzare il SSID. Il SSID viene in genere visualizzato nell'elenco delle reti disponibili, semplificando l'identificazione della rete wireless in uso se ne è presente più di una nella stessa area.



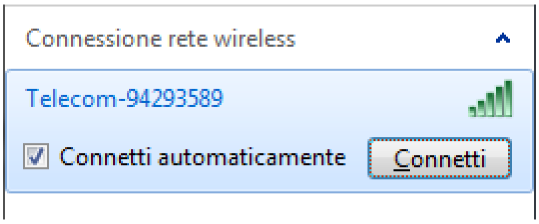
posizionare con attenzione il router o il punto di accesso: dato che il segnale wireless può essere trasmesso a diverse decine di metri, dalla rete potrebbe oltrepassare il perimetro della propria abitazione. È possibile limitare l'area raggiunta dal segnale wireless posizionando il router o il punto di accesso al centro della casa anziché vicino o esternamente a un muro o a una finestra.

Connettersi ad una rete wireless

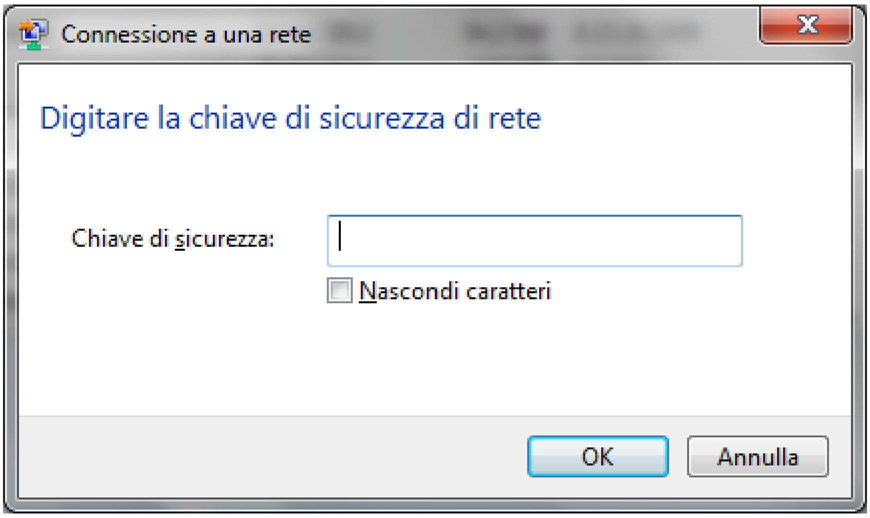
Se si dispone di un dispositivo wireless portatile, si può visualizzare l'elenco delle reti wireless disponibili nella zona dove ci si trova e connettersi a una di tali reti.
Nel caso di Windows 7, per visualizzare l'elenco delle reti wireless disponibili, si deve cliccare sull'icona della rete nell'area di notifica, accanto all'orologio di Windows.



A questo punto si può selezionare il nome della rete wireless a cui collegarsi.



Se si vuole che Windows si connetta automaticamente alla rete Wi-Fi selezionata ogni volta che questa è disponibile e ne ricordi la password di accesso, mettere il segno di spunta accanto alla voce **Connetti automaticamente** prima di avviare la connessione.



Se la rete e protetta, è necessario disporre della chiave di sicurezza di rete. Digitare la password impostata per la connessione nel campo **Chiave di sicurezza** e cliccare su **OK**. Se la password è corretta, al termine della procedura, viene segnalato che la connessione alla rete senza fili e stata stabilita.
In maniera predefinita, Windows memorizza le password delle connessioni Wi-Fi e si connette automaticamente a queste ultime quando il livello del segnale lo permette.
Ricordiamo che entrare in una rete WiFi (protetta o libera) senza il benestare del proprietario, carpendo in modo fraudolento la chiave di sicurezza, è un reato perseguibile a termini di legge.

Domande

1. Un hotspot WiFi
    a. È un punto di accesso ad internet, con tecnologia cablata, aperto al pubblico
    b. È un punto di accesso ad internet, con tecnologia cablata, non aperto al pubblico
    c. È un punto di accesso ad internet, con tecnologia wireless, aperto al pubblico
    d. È un punto di accesso ad internet, con tecnologia wireless, non aperto al pubblico
2. Quale tipo di rete offre maggior sicurezza?
    a. Una rete WiFi
    b. Una rete cablata
    c. Entrambe offrono la stessa sicurezza
    d. Tutte le affermazioni sono errate
3. Quale tipo di rete è più vulnerabile ad accessi non autorizzati?
    a. Una rete WiFi
    b. Una rete cablata
    c. Sono vulnerabili nello stesso modo
    d. Tutte le affermazioni sono errate
4. Cosa si intende con SSID?
    a. La chiave di sicurezza della rete
    b. Il segnale identificativo della rete
    c. La password di rete
    d. Tutte le affermazioni sono errate
5. Quale tipo di chiave di sicurezza offre maggiori garanzie?
    a. Chiave WEP
    b. Chiave WPA
    c. Chiave WPA-PSK
    d. Sono tutte equivalenti
6. Come si chiama il codice che permette di identificare univocamente il dispositivo dotato di connettività Internet?
    a. SSID
    b. WPA
    c. MAC
    d. WEP
7. Quale dei seguenti indirizzi IP è meno “sicuro”?
    a. 192.168.1.1
    b. 188.158.34.12
    c. 203.168.111.110
    d. 200.148.131.120
8. Come è chiamata la sequenza di caratteri che si deve scrivere per connettersi in un’area protetta?
    a. Password
    b. Codice Segreto
    c. Chiave di sicurezza
    d. Codice di attivazione

9. Quale tra i seguenti non è uno standard di sicurezza per le reti Wi Fi?
    a. WEP
    b. WPA
    c. WAP
    d. Tutte le risposte sono errate
10. Dove si trova l’icona relative alle connessioni di rete in Windows 7?
    a. Nella System Tray
    b. Nell’area di notifica
    c. Vicino all’orologio nella barra
    d. Tutte le risposte sono esatte

Capitolo 9

Controllo degli accessi

Regolare gli accessi alla rete

Nella gestione di una rete è fondamentale che l'amministratore regoli e controlli gli accessi alle informazioni e alle risorse della stessa da parte degli utenti: per due motivi:

1. controllare che l'accesso avvenga solo da parte di utenti autorizzati;
2. regolare l'utilizzo delle risorse e delle informazioni presenti nella rete a seconda dell'utente.

Account di rete

Abbiamo accennato come l'amministrazione di rete implichi responsabilità maggiori rispetto alla semplice installazione e risoluzione dei problemi hardware. In particolare, una volta che l'hardware è installato e configurato, l'amministratore deve verificare che gli utenti possano accedere alle risorse che sono autorizzati a utilizzare.

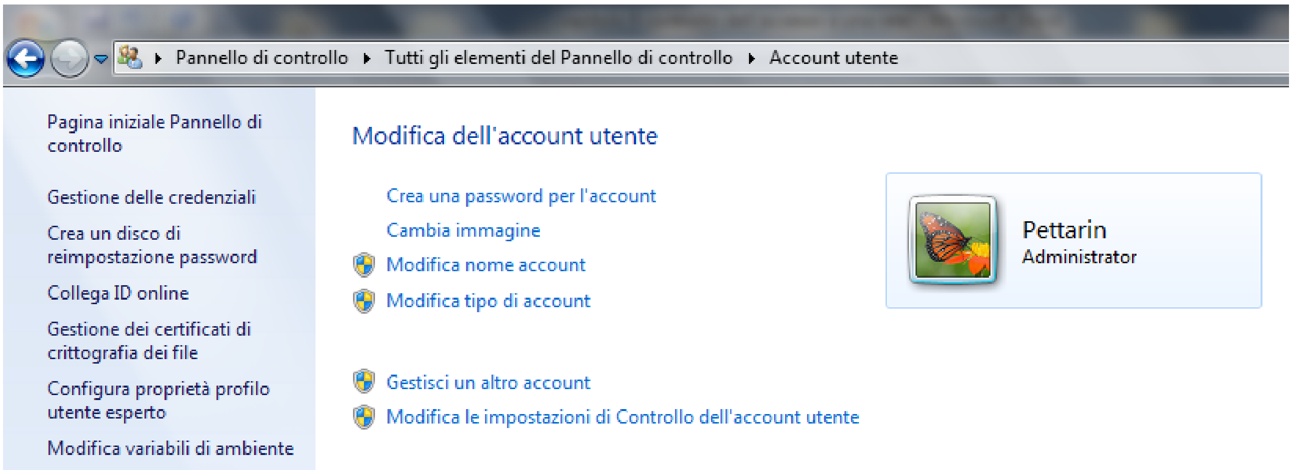
È quindi necessario che ciascun utente di una rete sia in possesso di un **account di rete**: sono delle credenziali personali (nome utente e password) che permettono all'utente di accedere alla rete e utilizzare le risorse che l'amministratore ritiene opportuno concedergli.

L'accesso a un account è un processo chiamato *login* (o *logon*): è una procedura di riconoscimento, detta autenticazione, dove sono richieste le credenziali d'accesso, il nome utente (*username*) e la *password* (parola d'ordine).

Lo username dovrebbe consentire un riconoscimento del tipo di utente: amministratore, ospite (guest), segreteria, ecc. Lo username, può essere noto a tutti ed è sempre noto all'amministratore del sistema. La password, invece, è un'informazione rigorosamente attribuita al possesso dell'utente, che ne è unico responsabile.

I sistemi Windows sono multiutente: consentono di creare e gestire diversi account Windows sulla stessa macchina, ognuno di essi accederà al sistema a mezzo delle credenziali.

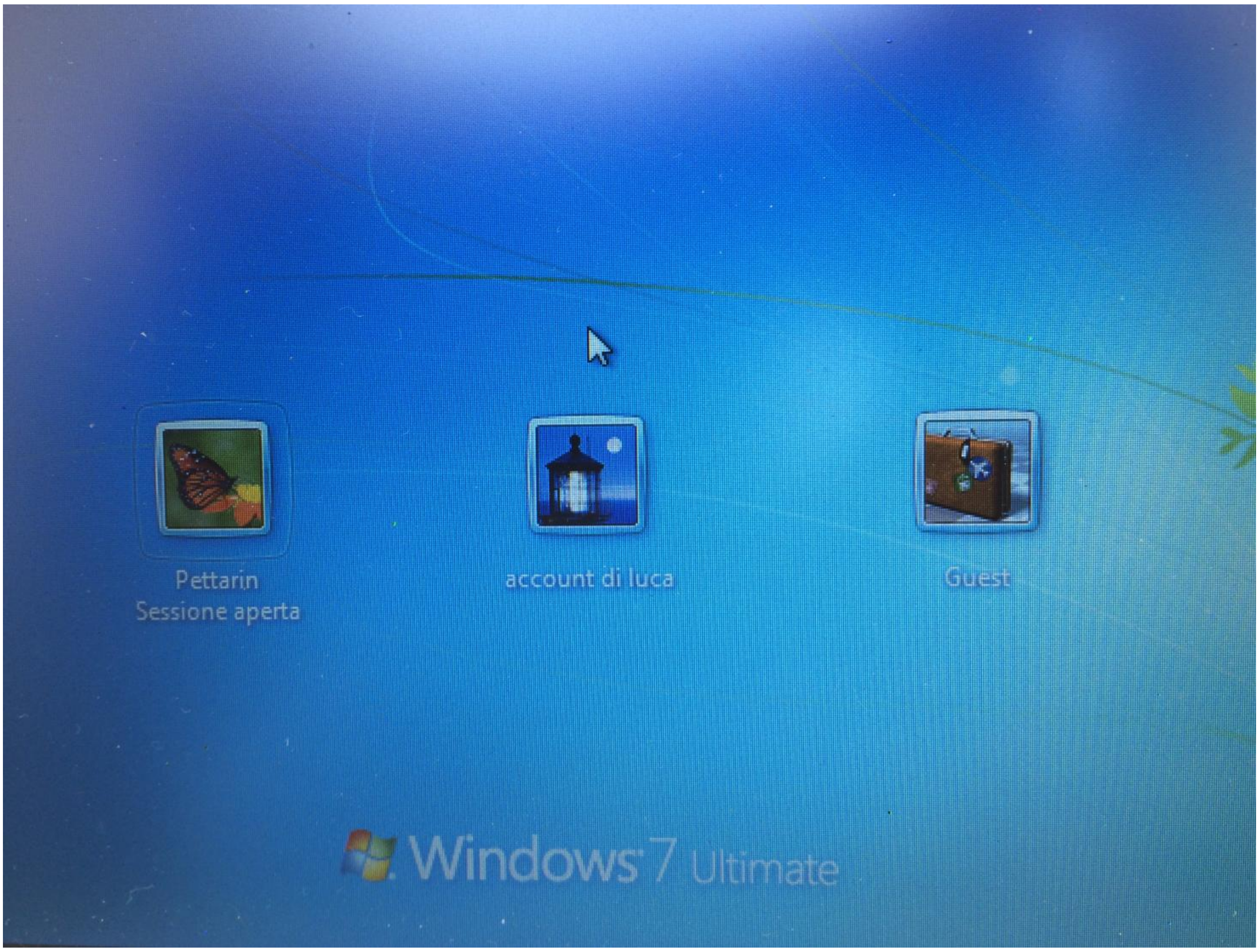
Per creare, modificare o cancellare un account utente in Windows, nel **Pannello di Controllo** si seleziona **Account Utente**.



Attraverso un Wizard si può procedere alla creazione e gestione di ogni account presente nella macchina.

L'account di livello più elevato è **Administrator**: con questo account si può eseguire qualsiasi operazione sul computer o sulla rete: cambiare e modificare password, installare e disinstallare programmi, aprire e modificare qualsiasi file o cartella, cancellare o creare altri account. In Windows deve essere presente almeno un'utente con permessi d'amministratore.

Quello a livello più basso è **Guest**: per questo account non è prevista la password e consente l'accesso solo temporaneo ad ospiti.



L'accesso alla rete dipende dalla sua architettura. Ci possono essere reti di tipo **paritetico** dove non ci sono server sulla rete. Ogni computer funge contemporaneamente da client e da server e tutti i computer svolgono funzioni simili. L'autenticazione degli utenti avviene a livello locale: è il caso di piccoli uffici dove ogni pc è autosufficiente, dotato di propria stampante e di ogni altro dispositivo necessario. L'addetto al computer è sia amministratore che utente.
Nelle reti **client/server** il *server*, cioè il computer che offre le proprie potenzialità a tutti gli altri computer (*client*) connessi alla rete, gestisce l'autenticazione degli utenti su tutti i client e centralizza i permessi di accesso alle risorse di tutta la rete.

Politiche per la scelta e la gestione delle password

Scegliere una password adeguata alla sicurezza informatica richiesta è importantissimo. Una password "robusta" è il migliore strumento per proteggere le informazioni personali. Per quanto ci possa sembrare sicura e impenetrabile, ci sono diversi sistemi a disposizione per forzare una password:

1. **un attacco "a forza bruta" (brute-force)**: mediante software che tentano di risalire a una password provando tutte le combinazioni possibili oppure con un attacco "a dizionario", utilizzando un elenco di termini usuali;
2. **tecniche di phishing o di "ingegneria del sociale"**; questi sistemi utilizzano soprattutto messaggi di posta elettronica fasulli o messaggi istantanei, ma anche contatti telefonici, che ingannano l'utente portandolo a rivelare i propri dati personali;
3. **installare programmi in grado di trafugare informazioni**: per prevenire questo tipo di attacchi può servire un buon antivirus e un firewall.

Come abbiamo già detto, per avere delle minime caratteristiche di sicurezza, una password:

1. deve essere piuttosto lunga e dovrebbe contenere non meno di 8 o 10 caratteri. La lunghezza ideale è dai 14 caratteri in su;
2. deve contenere una serie di numeri, lettere (maiuscole e minuscole), e magari caratteri diversi tipo # @. Un eventuale attacco brute-force dovrebbe provare un grande numero di combinazioni;
3. non utilizzare la data di nascita, la targa dell'auto, il numero del cellulare o qualunque altro dato personale facilmente individuabile;
4. non inserire una serie di numeri o caratteri ripetuti o composte da lettere (e numeri) che nella tastiera sono vicine;
5. non utilizzare la stessa password per più account;
6. modificare periodicamente la password: comunque la complessità della password garantisce la sicurezza nel tempo. Una password con 14 o più caratteri può essere utilizzata per molti anni.

Tecniche di sicurezza biometriche

In alcuni casi, al posto delle password, per accedere al computer in modo sicuro vengono utilizzati dei sistemi che si basano su **tecniche biometriche**: sono delle tecniche che permettono di identificare una persona sulla base di una o più caratteristiche fisiche.
Le tecniche biometriche più comuni sono:

1. **riconoscimento vocale**: il riconoscimento della voce è una delle tecniche biometriche più utilizzate. Si rileva il timbro, la tonalità e la velocità con cui si parla;

2. **lettore impronte digitali**: un lettore di impronte digitali riesce a diversificare le diverse improntì umane che sono tutte una diversa dall'altra. Questa tecnologia è già presente in diversi computer portatili, cellulari, ecc.;



3. **scansione dell'iride dell'occhio**: questi sistemi di controllo funzionano tramite la lettura ed il riconoscimento dell'iride umana. Una speciale telecamera, in un paio di secondi, fa la scansione dell'iride. Dopo aver fotografato l'occhio, il sistema elabora le possibili variazioni dovute alla luce e salva l'immagine digitale in un apposito database. In seguito l'utente dovrà soltanto guardare nella stessa telecamera e il controllo dell'iride avverrà in meno di un secondo. I costi di questa tecnologia sono ancora abbastanza elevati.



Domande

1. Quale password è più sicura?
    a. Meida
    b. Dtst
    c. Buc123
    d. Whapdfr_69
2. Quali sono tecniche biometriche che permettono di identificare una persona?
    a. Riconoscimento vocale
    b. Lettore impronte digitali
    c. Scansione dell'iride dell'occhio
    d. Tutte le affermazioni sono corrette
3. In Windows qual è l’account di livello più elevato?
    a. Administrator
    b. Guest
    c. Sono allo stesso livello
    d. Tutte le affermazioni sono errate

Capitolo 10

Uso sicuro del web

Navigare in siti sicuri

La rete internet, inizialmente, era concepita come strumento di ricerca di informazioni. L'utente esercitava un ruolo passivo. Non interagiva con le pagine web ma si limitava al reperimento e alla consultazione dei dati di suo interesse. Da parecchi anni, con l'avvento del Web 2, l'utente di internet è diventato attivo: pubblica materiale proprio, inserisce informazioni, effettua acquisti, ecc. Addirittura gestisce il proprio conto bancario.
È evidente che tutto questo richiede che le pagine web dove si effettuano queste operazioni devono garantire un livello di sicurezza elevato per prevenire il furto di informazioni così rilevanti.

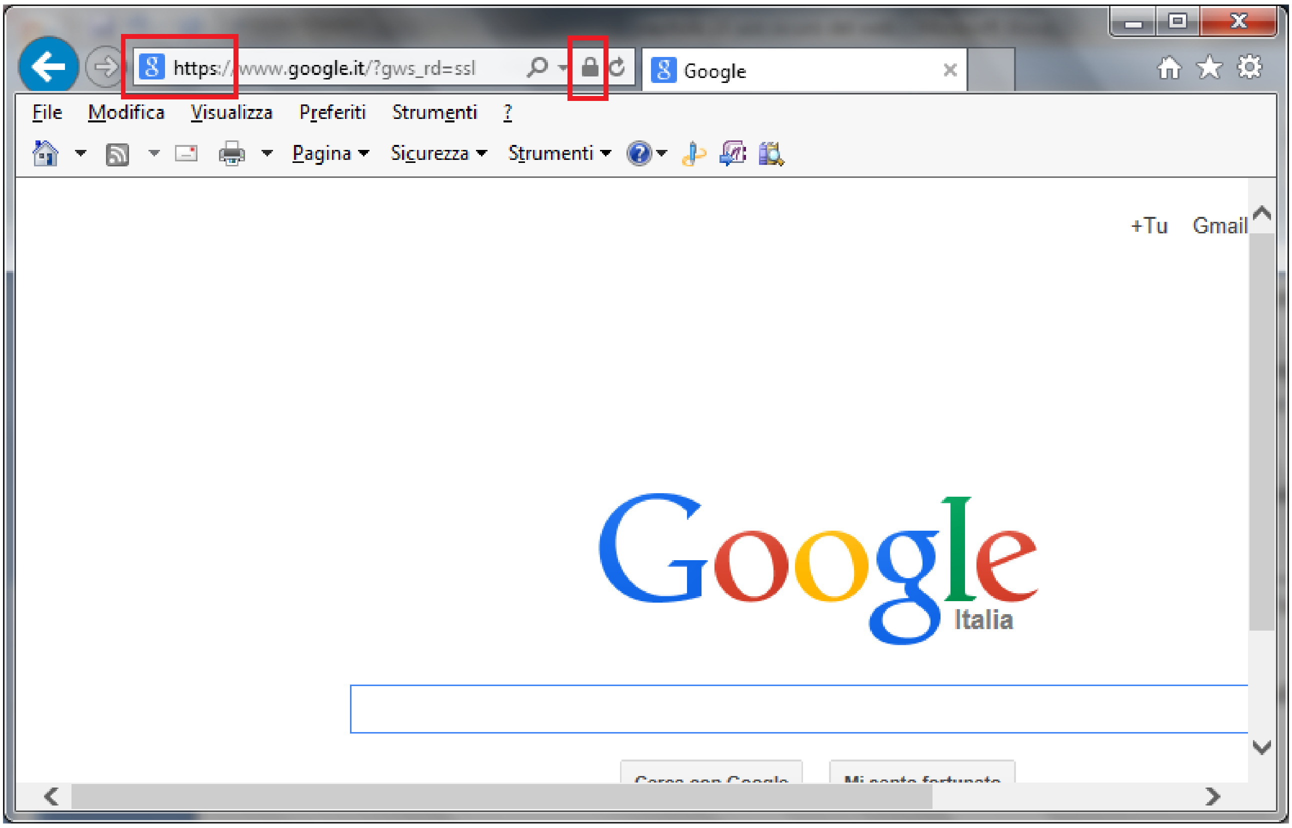
Identificazione di un sito web sicuro. I certificati digitali

Ci sono dei siti internet impostati in modo da impedire l'accesso da parte di utenti non autorizzati: ad esempio siti di home banking, acquisti on line, registrazione esami universitari, ecc.
Questi siti Web sono denominati **protetti**. La protezione avviene con l'utilizzo dei **certificati**.
Un certificato è un documento digitale che consente di verificare l'identità di una persona o un sito web. I certificati vengono rilasciati da società denominate **Autorità di certificazione**. Queste autorità stabiliscono e verificano l'autenticità delle chiavi pubbliche appartenenti a persone o altre autorità di certificazione e verificano l'identità di una persona o organizzazione che richiede un certificato.
Ci sono due tipi di certificati:

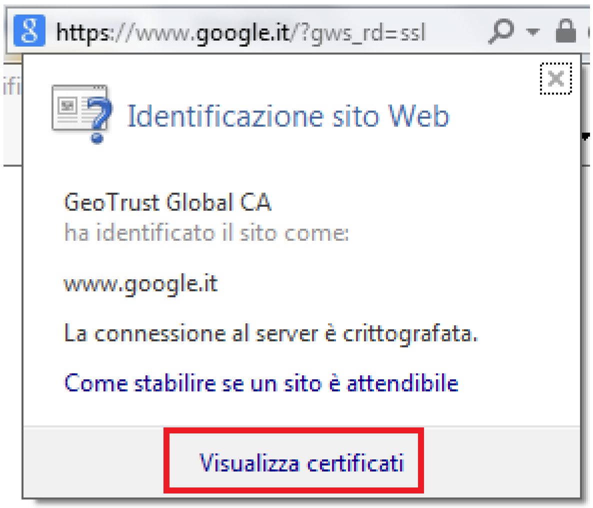
1. Un certificato personale consente di verificare l'identità dell'utente e viene utilizzato quando si inviano informazioni personali tramite internet a un sito web che richiede un certificato per verificare l'identità dell'utente. È possibile provare la propria identità con una chiave digitale privata di tipo hardware o software.
2. Un certificato di un sito web consente di identificare l'autenticità di un sito web specifico e di verificare che l'identità del sito protetto originale non venga assunta da un altro sito web. Quando si inviano informazioni personali in internet, è opportuno controllare il certificato del sito web per assicurarsi di comunicare con il sito previsto.

I certificati sono generalmente forniti agli utenti in automatico quando si utilizza un sito web sicuro per transazioni commerciali o bancarie online o si desidera crittografare un file. Se si desidera un certificato per uso personale, ad esempio per proteggere la posta elettronica mediante una firma digitale, si può contattare un'autorità di certificazione e richiedere un certificato.
Riassumendo, i certificati sono principalmente utilizzati per verificare l'identità di una persona o per autenticare un servizio.

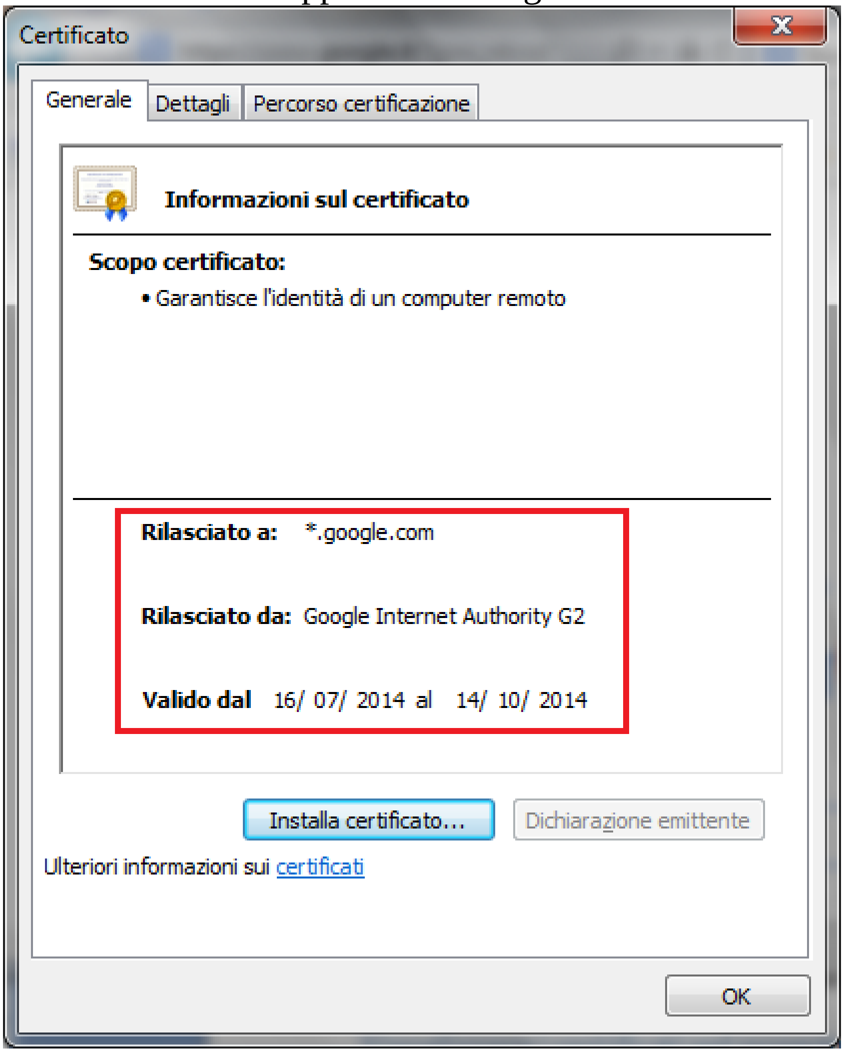
Quando si visita un sito Web protetto, il sito invia automaticamente il proprio certificato all'utente, crittografando (cioè scrivendo le informazioni in modo cifrato) le informazioni.
In Internet Explorer, nel caso di sito protetto, è visualizzata un'icona a forma di lucchetto nella barra degli indirizzi. In figura la pagina web di Google.



L'indirizzo della pagina inizia con la sigla **https** (Hyper Text Transfer Protocol Secure), invece che il "classico" http. Significa che il sito trasmette i dati dopo averli cifrati con una chiave robusta in modo che il solo sito web che li riceve e li trasmette sia in grado di decodificarli. La "s" significa "sicuro".
Facendo clic sul lucchetto, appare il rapporto sulla sicurezza relativo al sito Web con le informazioni contenute nel certificato.



Con un clic su **Visualizza certificati** appaiono i dettagli della certificazione.

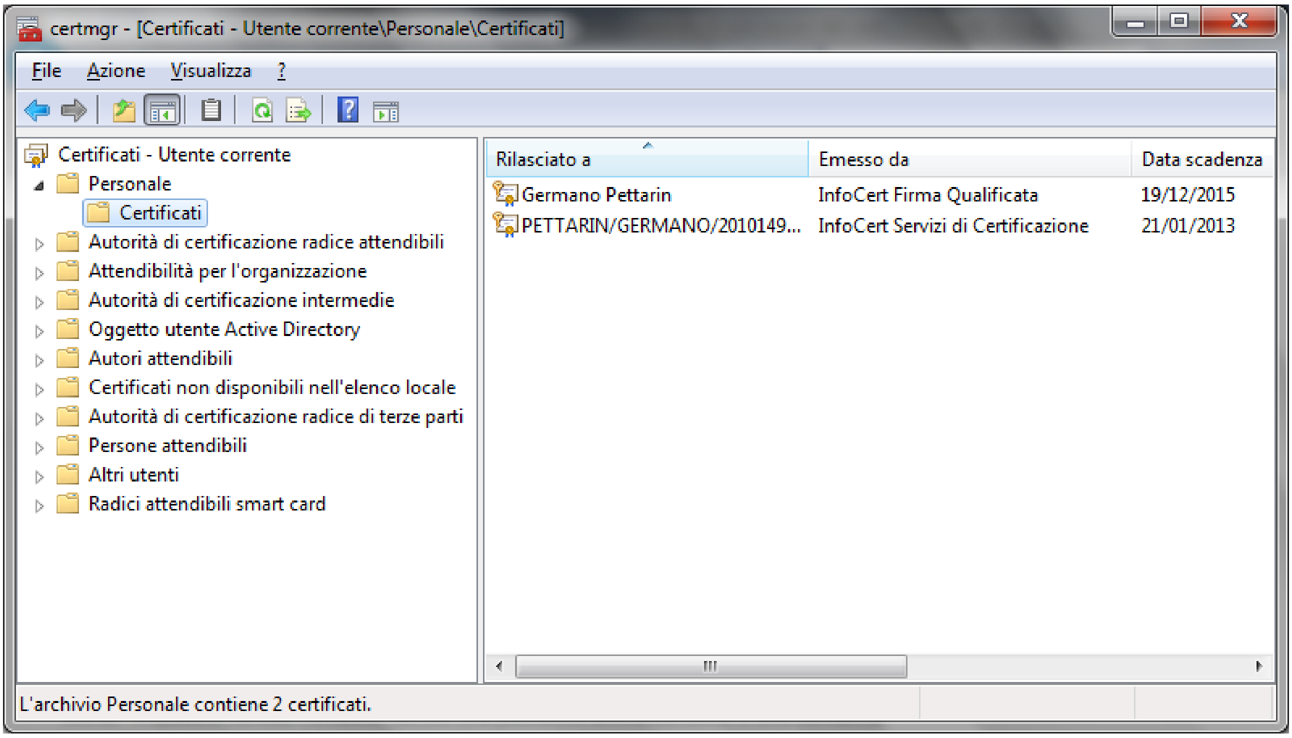


Sono specificate le informazioni di identificazione dell'autorità di certificazione e la data di inizio e la data di fine della validità, che rappresentano i limiti del periodo di validità. Un certificato è valido esclusivamente per il periodo specificato. Trascorso il periodo di validità, il soggetto del certificato scaduto dovrà richiederne uno nuovo.

Visualizzare i certificati nel proprio computer

È possibile visualizzare i certificati presenti nel computer con il **Gestore certificati**: è necessario essere connessi al computer come amministratore.

Per aprire Gestore certificati, fare clic sul pulsante **Start**, digitare **certmgr.msc** nella casella di ricerca e premere INVIO. Può essere richiesta una password amministratore o una conferma.



Il Pharming

Il **pharming** è una tecnica per impadronirsi dei dati personali di un utente, principalmente i dati bancari, simile al **phishing**.
Nel caso del pishing si hanno delle e-mail (o SMS) con falsa intestazione della banca, contenenti un link di collegamento a un "sito clone" (apparentemente identico al sito originale) e la richiesta di accedervi con le motivazioni più disparate: un movimento bancario non autorizzato, la verifica dell'estratto conto, un bonifico da confermare, ecc. Se si clicca sulla richiesta, appare una falsa pagina di accesso al conto corrente online, del tutto simile a quella vera. I dati saranno registrati dai truffatori per poi accedere al conto e ed effettuare operazioni illecite. Per raggiungere il maggior numero possibile di utenti, la stessa falsa e-mail (o SMS) è inviata a moltissimi indirizzi diversi, di clienti e non clienti, in maniera simultanea e pressoché casuale.
Nel pharming quando si digita l'indirizzo web della propria banca, o si clicca sul relativo link, si viene indirizzati in automatico al sito "clone" anche in questo caso, nel momento in cui si inseriscono i dati bancari personali, i truffatori li copiano per utilizzarli in un secondo tempo per operare sul conto corrente.
Questa tecnica opera associando all'indirizzo alfanumerico del sito un indirizzo IP diverso, quello del sito "clone". L'utente non ha strumenti per rendersi conto della differenza se non controllare il certificato digitale della pagina che utilizza il protocollo https.

One-time password

Come si intuisce dalla traduzione in italiano, una **One-Time Password** (password usata una sola volta, OTP) è una password che è valida solo una volta, per una singola sessione di accesso o una singola operazione. Gli algoritmi di generazione delle OTP in genere fanno uso di numeri casuali.
Utilizzando una OTP si possono evitare i problemi di violazione di una tradizionale password statica. Abbiamo visto come quest'ultima possa essere forzata con attacchi a forza

bruta, con software che generano tutte le possibili combinazioni di numeri e lettere. Nel caso delle OTP, dato che il valore è continuamente modificato, se un malintenzionato riesce ad conoscere una OTP già utilizzata per accedere a un servizio o eseguire una transazione, non può utilizzarla, in quanto non è più valida.
Chiaramente una OTP non può essere creata e memorizzata da una persona. Di solito, si usa un dispositivo elettronico di dimensioni ridotte (token OTP) con un display che visualizza la password generata di volta in volta.



Normalmente la OTP è una password aggiuntiva al nome utente e password utilizzati per accedere a un servizio.



Domande

1. I certificati sono principalmente utilizzati per:
    a. Verificare l'identità di una persona o per autenticare un servizio
    b. Proteggere l’accesso a una rete
    c. Generare delle chiavi di sicurezza
    d. Tutte le affermazioni sono errate
2. Una transazione finanziaria può essere effettuata anche in una pagina Web senza l’icona del lucchetto
    a. No, non è possibile
    b. Si può fare ma non è sicuro
    c. Il lucchetto è una icona inutile
    d. Non esiste alcuna icona a forma di lucchetto
3. La sigla http significa
    a. Hyperlink TransiT Protocol
    b. HyperType Tweet Protocol
    c. HyperText Transfert Protocol
    d. Tutte le risposte sono errate
4. Esiste un tipo di attacco informatico che consiste nel dirottare il traffico di un sito web verso un clone contraffatto. Si chiama:
    a. trojan
    b. pharming
    c. pishing
    d. worm
5. Cosa significa OTP?
    a. On That PC
    b. On Tera Pitch
    c. One Touch Ping
    d. One Time Password
6. Quale termine indica il servizio bancario online?
    a. E-cashing
    b. E-trading
    c. E-banking
    d. E-commerce
7. Pishing e Pharming sono sinonimi
    a. Vero
    b. Falso
    c. Il pishing non esiste
    d. Il Pharming non esiste
8. Il pharming è utilizzato solo per i siti web che gestiscono e-mail.
    a. È vero
    b. È falso
    c. È utilizzato solo per siti come i Social Network
    d. Il pharming non esiste

Capitolo 11

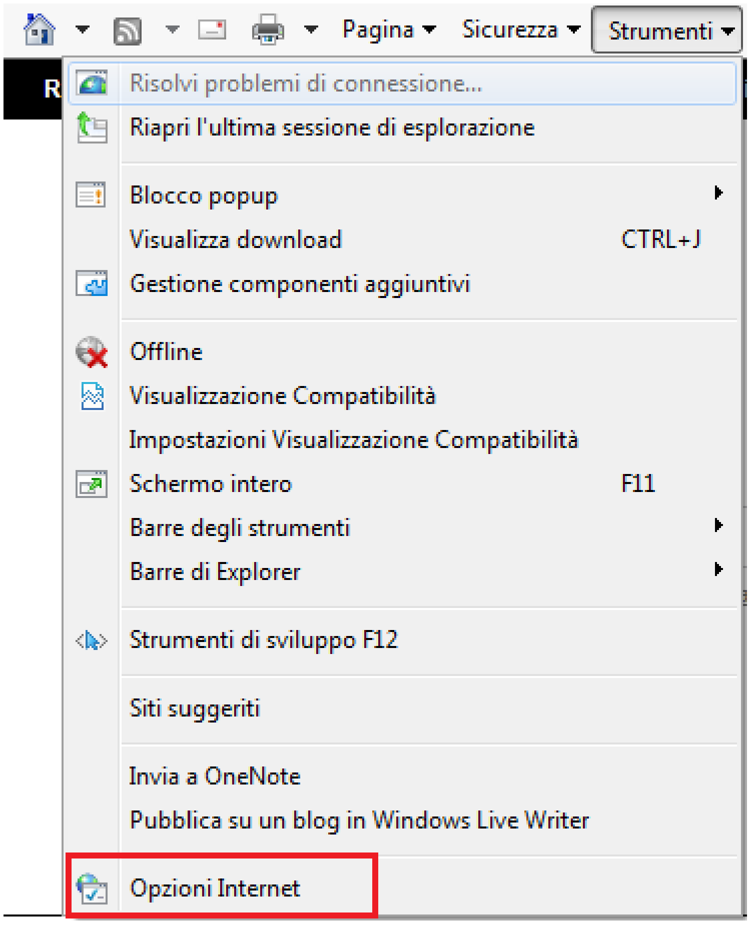
Impostare il browser per navigare in sicurezza

Opzioni di protezione

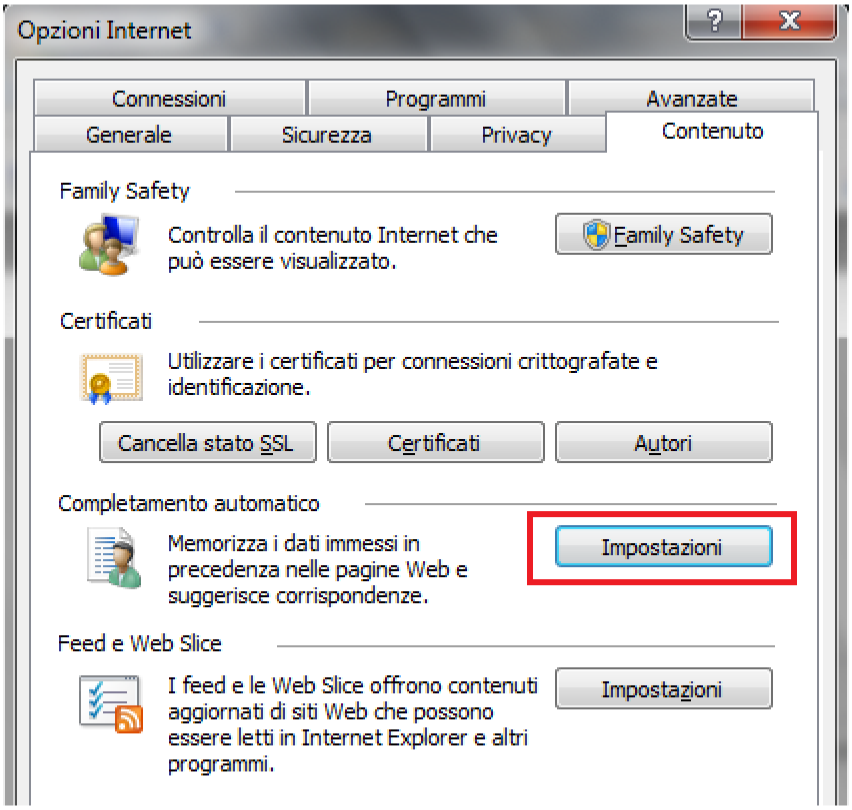
Data la crescente necessità di sicurezza e tutela dei propri dati durante la navigazione in rete, anche gli stessi browser si sono aggiornati, fornendo vari strumenti per tutelare i propri utenti. In questo capitolo facciamo riferimento al browser Internet Explorer 10.

Attivare/disattivare il completamento automatico dei dati

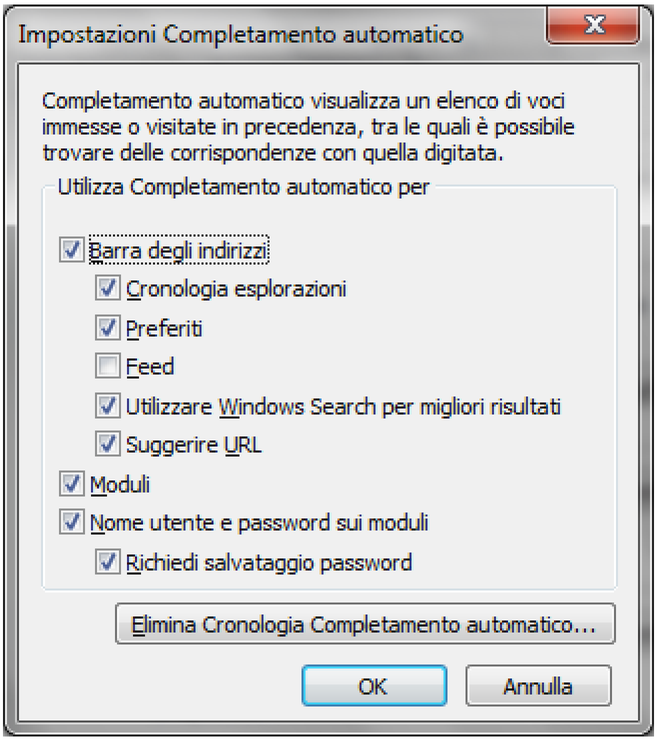
Quando si compila un modulo on line può capitare che il browser completi in modo automatico alcuni campi, proponendo dei valori inseriti in moduli simili o in navigazioni precedenti. È una opzione presente nel browser che gli consente di "ricordare" i dati inseriti e riproporli all'utente. È sicuramente una bella comodità, che evita la riscrittura di informazioni lunghe e complesse come il codice fiscale o il numero di cellulare.
Se il proprio computer è utilizzato da più utenti è conveniente disabilitare queste opzioni di completamento e di salvataggio automatico del browser, per evitare la diffusione dei propri dati personali.
Per disattivare il completamento automatico fare clic su **Strumenti** e scegliere **Opzioni Internet**.



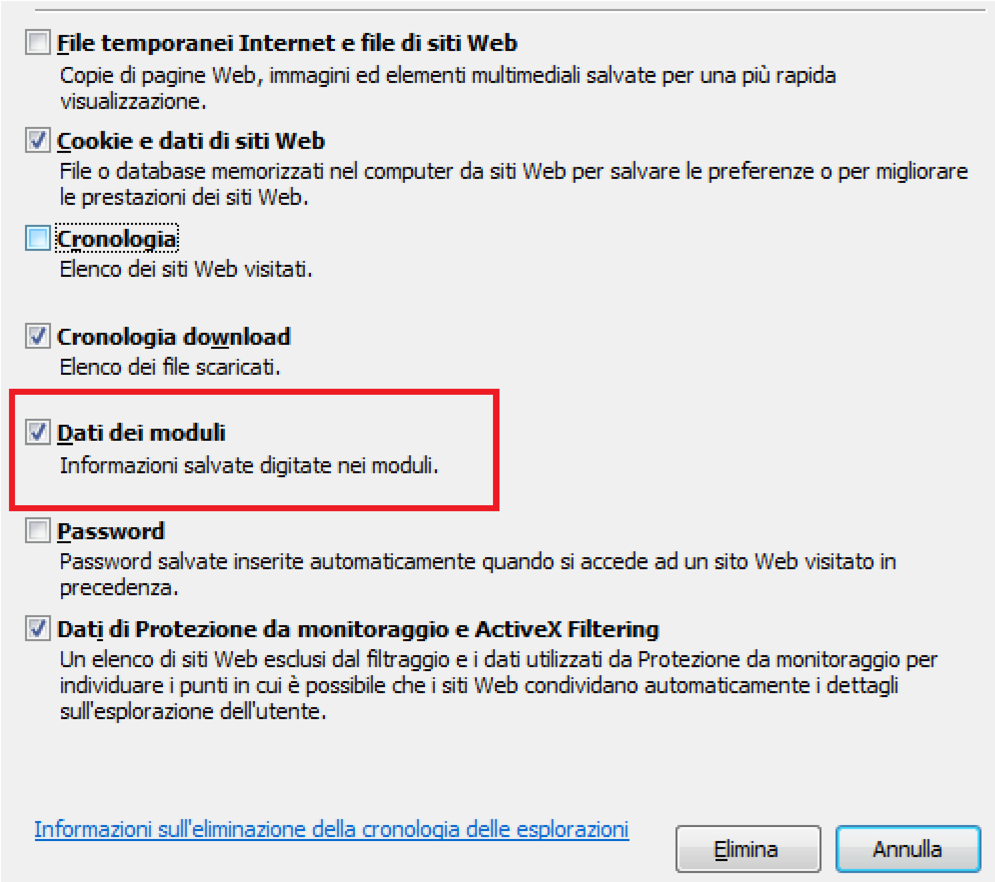
Nella scheda **Contenuto**, nel riquadro Completamento automatico, fare clic su **Impostazioni**.



Appare la finestra per le impostazioni del completamento automatico.



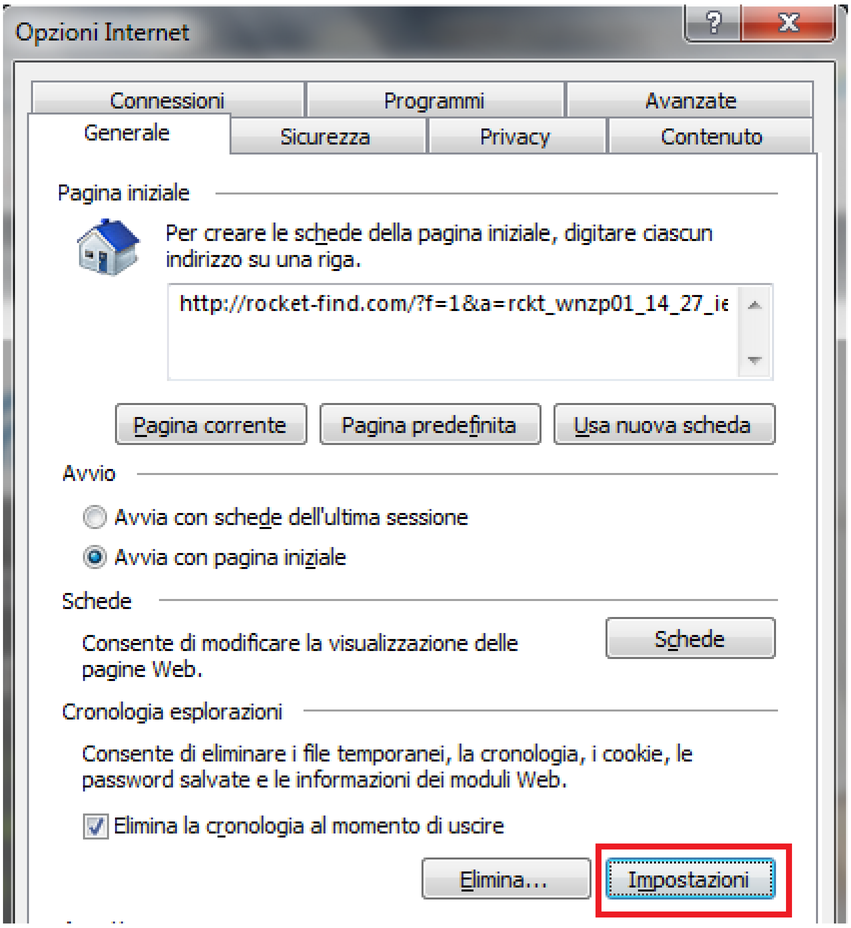
Per disattivare la memorizzazione delle informazioni inserite nei moduli è sufficiente disattivare la rispettiva casella. Per cancellare i dati memorizzati dal browser fare clic su **Elimina Cronologia Completamento automatico**.



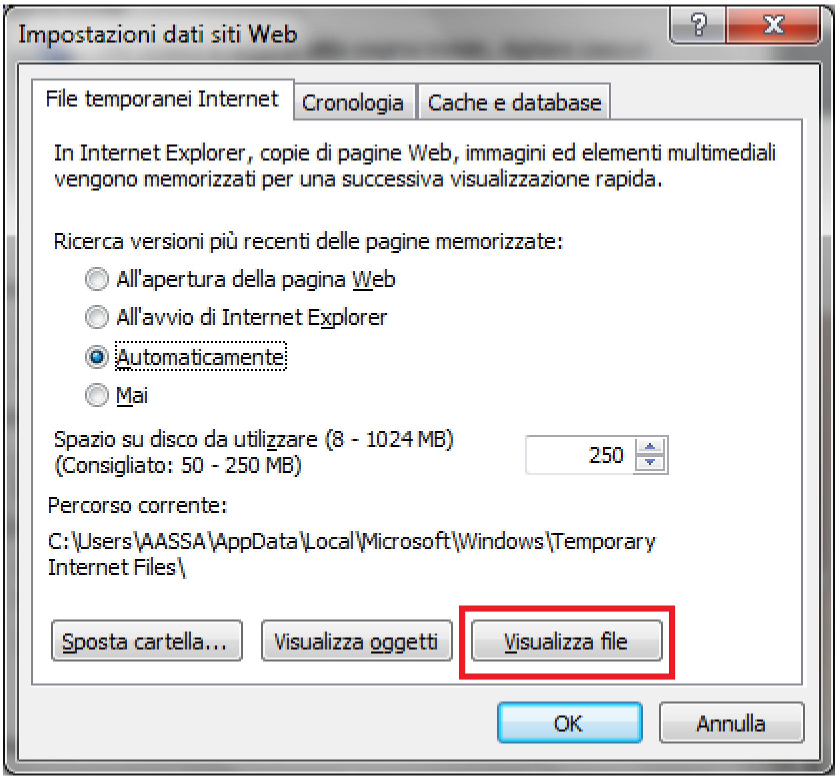
Appare l'elenco delle informazioni che il browser ha memorizzato durante le varie navigazioni. In particolare si possono eliminare i dati scritti nei moduli on line.

I cookie

I **cookie** ("biscotti") sono piccoli file di testo scritti dai siti web tramite il browser con lo scopo di memorizzare alcune informazioni utili a velocizzare un accesso successivo. Ad esempio i dati relativi agli acquisti fatti in un sito, le impostazioni di visualizzazione di una pagina web, ecc. Quando si accede nuovamente alla stessa pagina, il cookie viene inviato dal browser al server per automatizzare la ricostruzione dei propri dati.
L'elenco dei cookie memorizzati è visibile dalla finestra di **Opzioni internet** con un clic sul pulsante **Impostazioni** (scheda **Generale**).

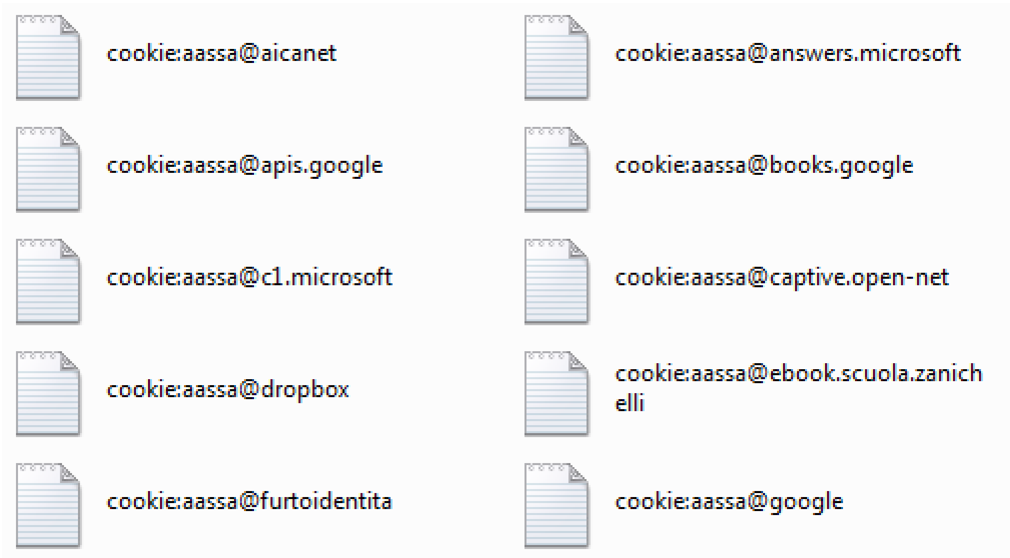


Appare la finestra per le **Impostazioni dati siti Web**.

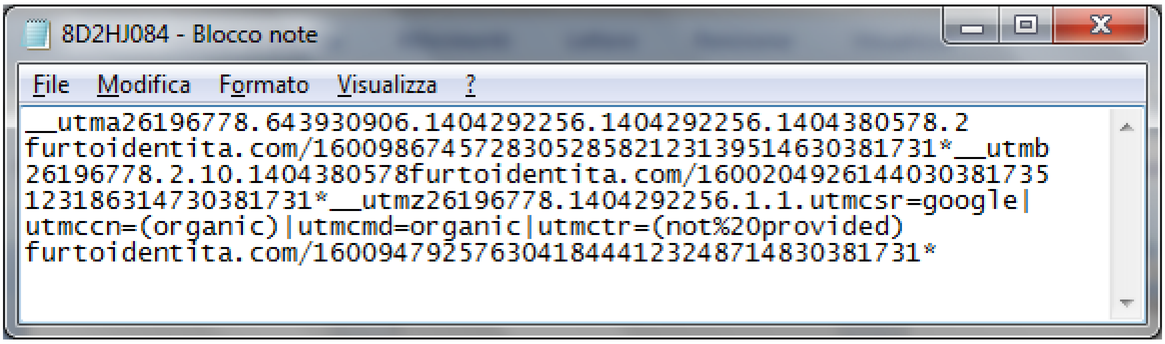


In questa finestra si può impostare come vengono cercate dal browser le versioni più recenti delle pagine memorizzate e quanto spazio del disco rigido viene utilizzato per memorizzare i

cookie e altri file temporanei di internet utili per velocizzare la navigazione. Questi file si possono visualizzare con un clic su **Visualizza file**.



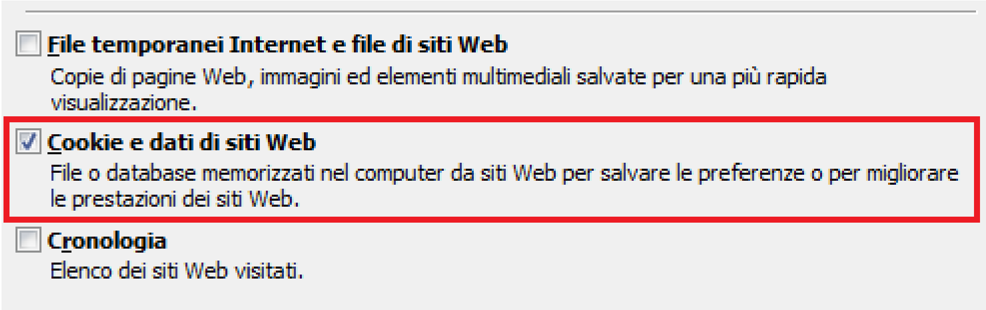
Come abbiamo detto, i cookie sono dei file di testo. Con un doppio clic si possono aprire (appare un messaggio per confermare l'apertura, dato che non sono file scritti dall'utente) e visionare il contenuto.



Il testo è codice per il server del sito, quindi non è comprensibile.
i cookie possono effettivamente contribuire a migliorare l'esplorazione consentendo al sito di raccogliere informazioni utili sulle preferenze dell'utente. Se è utilizzato in modo lecito è uno strumento utile. Ma può capitare che siano usati in modo illecito per tracciare i comportamenti degli utenti, come nel caso degli spyware. Inoltre i cookie possono costituire un rischio per la privacy in quanto tengono traccia dei siti visitati.

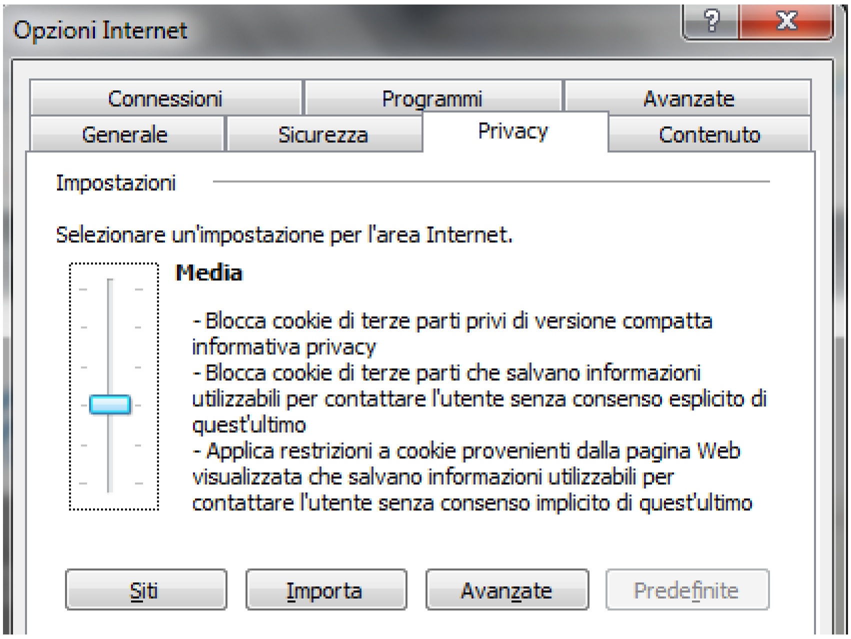
Eliminare i cookie

I cookie memorizzati si possono eliminare premendo il pulsante **Elimina** nella finestra **Opzioni internet** (scheda Generale). Appare l'elenco delle informazioni che il browser ha memorizzato durante le varie navigazioni, visto nel paragrafo precedente. Tra le varie opzioni ci sono anche i cookie.



Personalizzare le impostazioni dei cookie

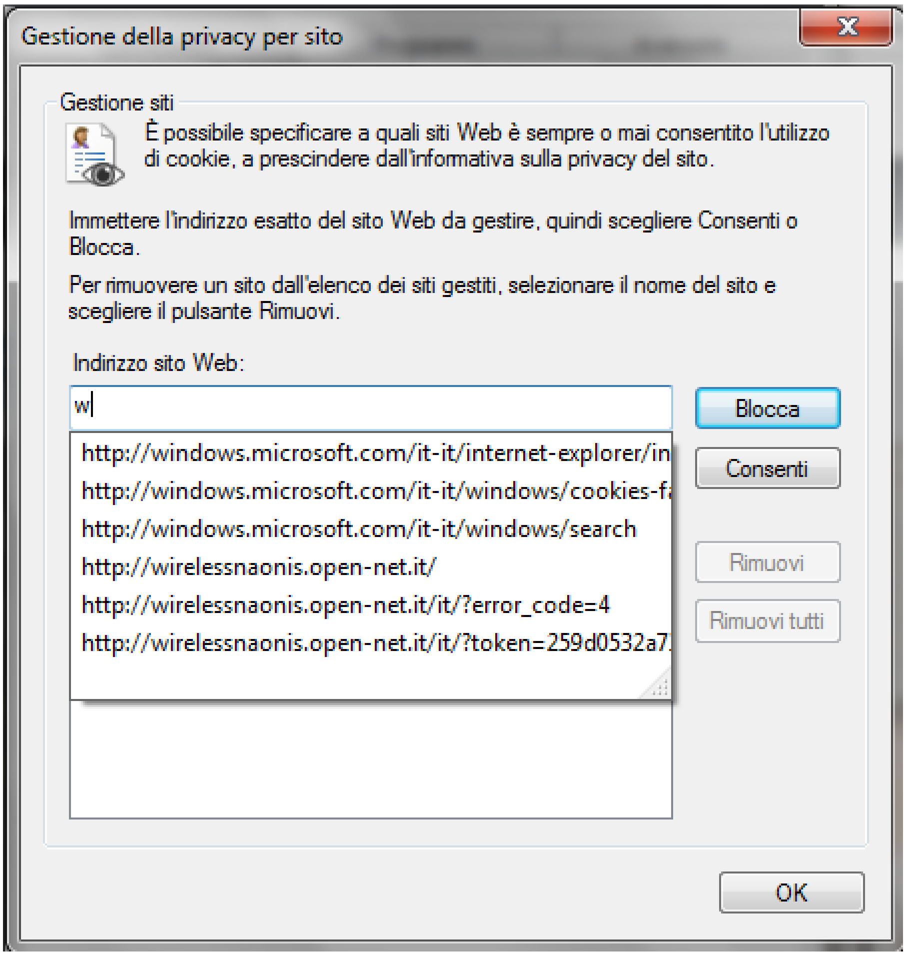
È possibile bloccare o consentire la memorizzazione dei cookie nella scheda **Privacy** della finestra **Opzioni internet**.



Spostando il dispositivo di scorrimento verso l'alto o verso il basso è possibile specificare tipi generici di cookie considerati accettabili. È ad esempio possibile scegliere di consentire i cookie di siti web che dispongono di informative sulla privacy e bloccare quelli di siti web che memorizzano informazioni personali senza il consenso dell'utente. Se si sposta il dispositivo completamente in alto si bloccano tutti i cookie. Completamente verso il basso si consente qualunque cookie.

Il blocco dei cookie potrebbe impedire la corretta visualizzazione di alcune pagine web.

In alternativa si possono consentire cookie da siti web specifici. Per prima cosa si deve spostare il dispositivo di scorrimento in una posizione intermedia in modo da non bloccare tutti i cookie o non consentirli tutti. Fare clic su **Siti**.



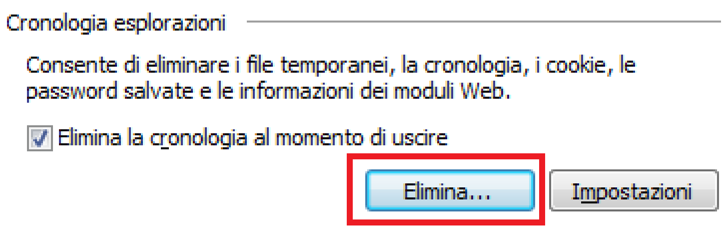
Nella casella **Indirizzo sito Web** digitare un indirizzo di sito web, quindi fare clic su **Blocca** o **Consenti**. Durante la digitazione dell'indirizzo, verrà visualizzato un elenco di pagine web già visitate. È possibile fare clic su una voce dell'elenco, che verrà visualizzata nella casella Indirizzo sito Web.

Ripetere il procedimento per ogni sito che si vuole bloccare o consentire. Al termine, fare clic su **OK** e riportare il dispositivo di scorrimento nella posizione originale.

Eliminare i vari dati privati da un browser

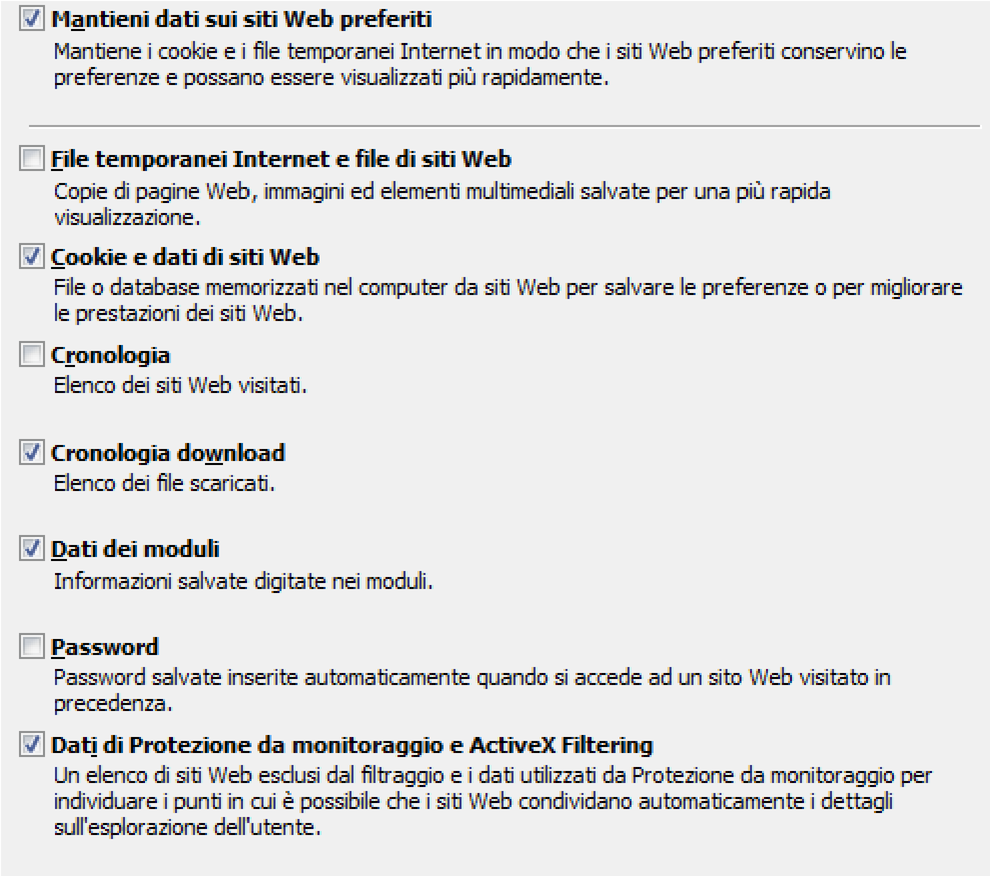
Nei paragrafi precedenti abbiamo visto come cancellare le informazioni private che il browser memorizza durante la compilazioni dei moduli.

Dalla stessa finestra è possibile eliminare tutte le altre informazioni personali sulle nostre sessioni di navigazione. Abbiamo visto che si può accedere alla finestra con il pulsante **Elimina** nella finestra **Opzioni internet** (scheda Generale).



In particolare è possibile eliminare i dati della **Cronologia**. La Cronologia contiene i collegamenti relativi ai siti Web visitati nella sessione corrente e nelle sessioni precedenti. In

realtà Internet explorer permette di ripulire questo elenco ogni volta che si chiude la sessione di navigazione con l'opzione **Elimina la cronologia al momento di uscire**.
La finestra **Elimina cronologia esplorazioni** permette di scegliere quali informazioni vogliamo cancellare.



Alcune delle opzioni le abbiamo già viste nei paragrafi precedenti. Le altre sono:

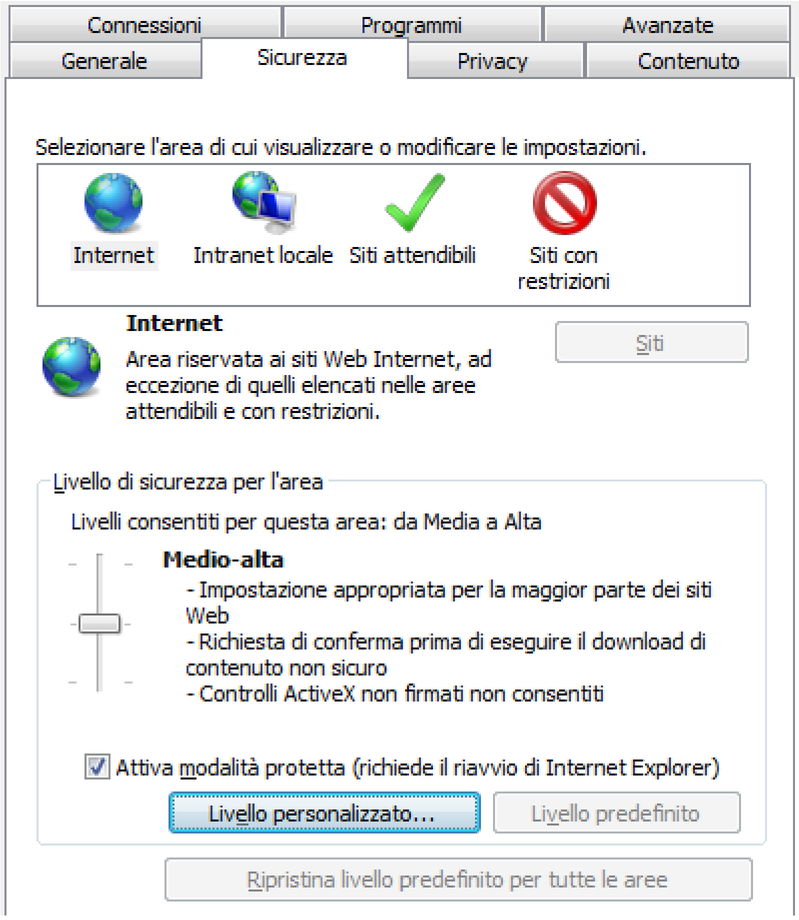
1. **File Internet temporanei**. Sono dei file relativi alle pagine web visitate la prima volta. Sono memorizzate nel computer per velocizzare un accesso successivo a queste pagine.
2. **Cronologia** delle pagine web visitate.
3. **Cronologia download**. Elenco dei file scaricati durante le sessioni di navigazione.
4. **Password** inserite in pagine con accesso protetto.
5. Dati di protezione da monitoraggio e ActiveX Filtering.

Selezionare le informazioni da cancellare e premere **Elimina**.
In particolare, eliminando la Cronologia, si cancellano le voci presenti nell'elenco della Barra degli indirizzi.
In particolare, l'opzione iniziale, **Mantieni dati sui siti web preferiti**, permette di mantenere i cookie e i file associati ai siti presenti nella lista Preferiti.

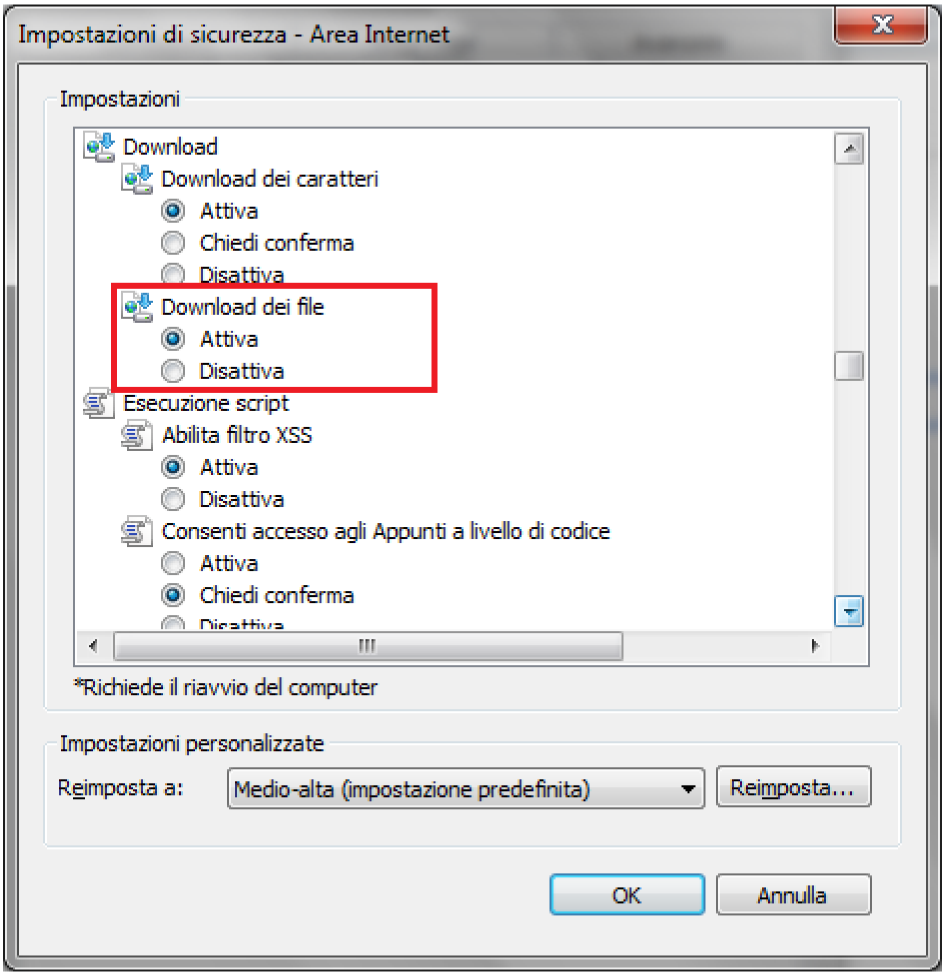
Controllo del contenuto dei siti

In ambito aziendale, esistono software che filtrano l'accesso a internet da parte degli utenti. Ad esempio, per impedire l'accesso a certi siti, come reti sociali, o semplicemente per limitare le operazioni che si possono effettuare in essi (scaricamento di file audio, video, eseguibili, in generale materiale protetto dai diritti d'autore),

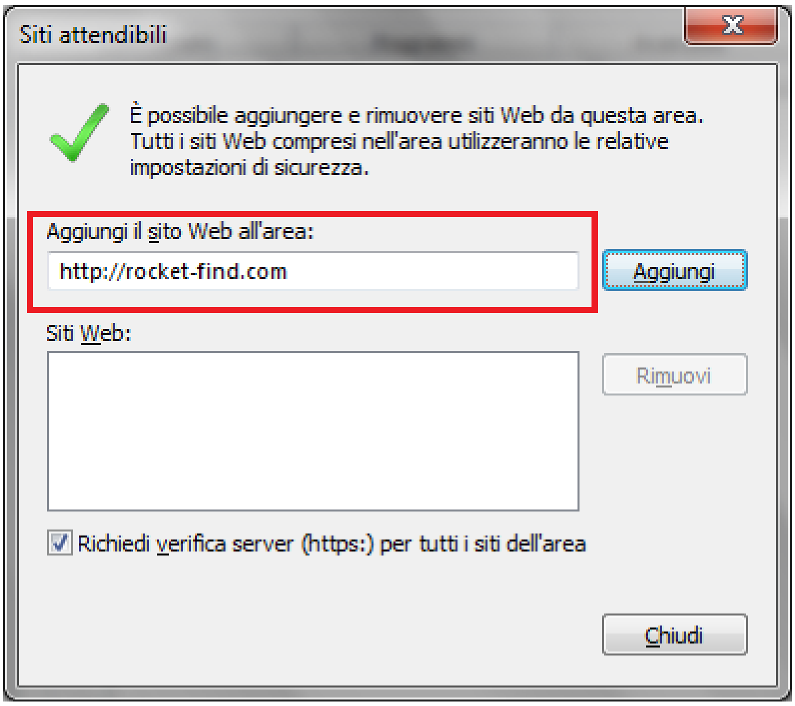
Internet Explorer permette, con la scheda **Sicurezza** in **Opzioni Internet**, di impostare restrizioni alle attività nei siti.



È possibile impostare quattro aree di sicurezza.
Internet: il livello di sicurezza per l'area Internet è applicato a tutti i siti web, ad esclusione di quelli specificati nelle altre aree. Il livello di sicurezza predefinito è Medio alto, ma può essere cambiato in Medio o Alto.
Intranet locale: quest'area riguarda i siti Web e il contenuto archiviato in una rete aziendale. Per i siti di quest'area (e successive) non è applicato il livello di sicurezza indicato nell'area Internet, ma quello dell'area: il livello predefinito è Medio.
Siti attendibili: in quest'area l'utente può indicare i siti che reputa attendibili e non pericolosi per il computer o per le informazioni. Il livello predefinito è Medio.
Siti con restrizioni: qui sono elencati i siti che potrebbero danneggiare il computer o le informazioni. I siti di quest'area non vengono bloccati, ma è impedito l'utilizzo di script o contenuto attivo. Il livello di sicurezza è impostato su Alto e non è modificabile.
È quindi possibile impostare una sicurezza alta ma includere alcuni siti web considerati sicuri ai siti attendibili: oppure, si può impostare una sicurezza bassa e includere siti pericolosi alla lista dei siti con restrizioni.
Per modificare le impostazioni per un'area di sicurezza, si sposta il dispositivo di scorrimento sul livello di sicurezza desiderato.
Si possono creare le impostazioni di sicurezza personalizzate per un'area con il pulsante **Livello personalizzato**. Ad esempio, disabilitare completamente i download.



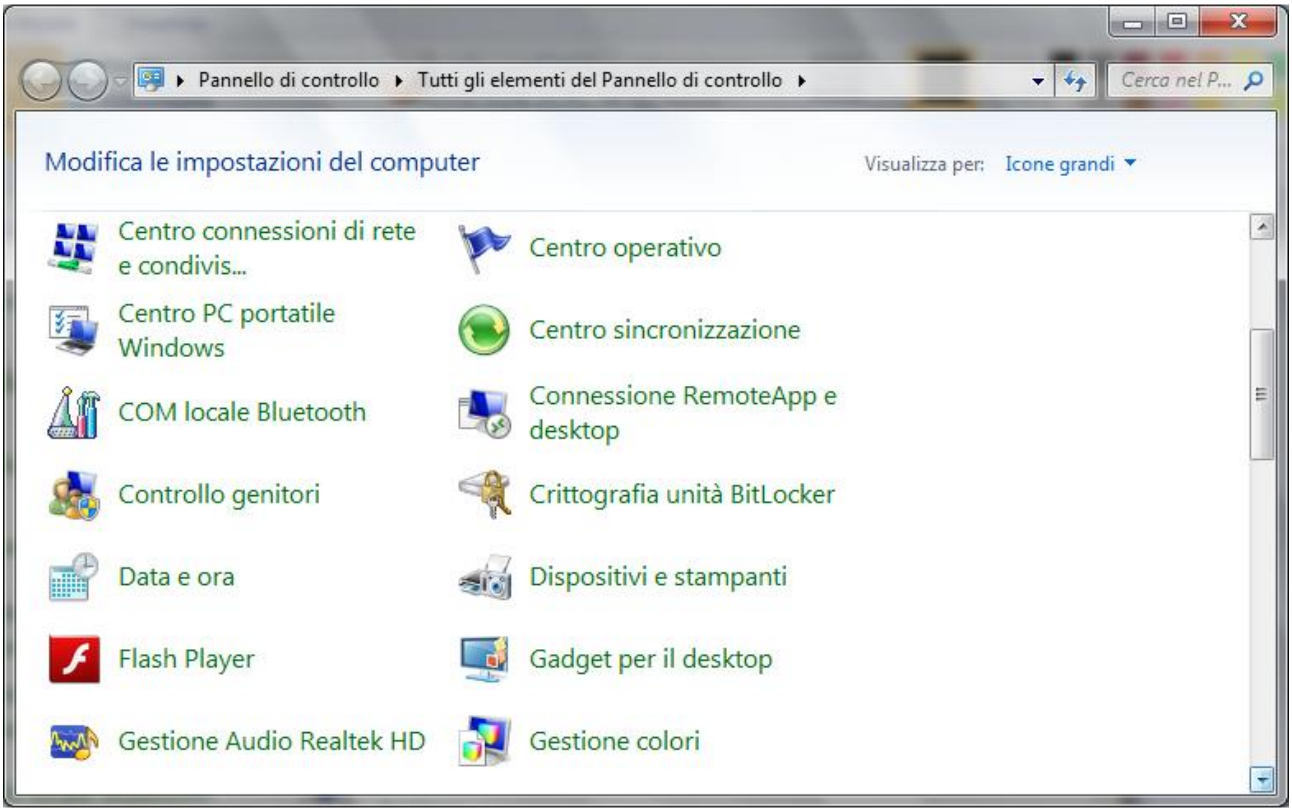
Per ripristinare le impostazioni originali di tutti i livelli di sicurezza, fare clic sul pulsante **Ripristina livello predefinito per tutte le aree**.
Per aggiungere un sito web a un'area di sicurezza, aprire il sito nel browser e selezionare un'area di sicurezza tra Intranet locale, Siti attendibili e Siti con restrizioni. Fare clic su **Siti**. Il sito Web verrà visualizzato nel campo **Aggiungi il sito Web all'area**.



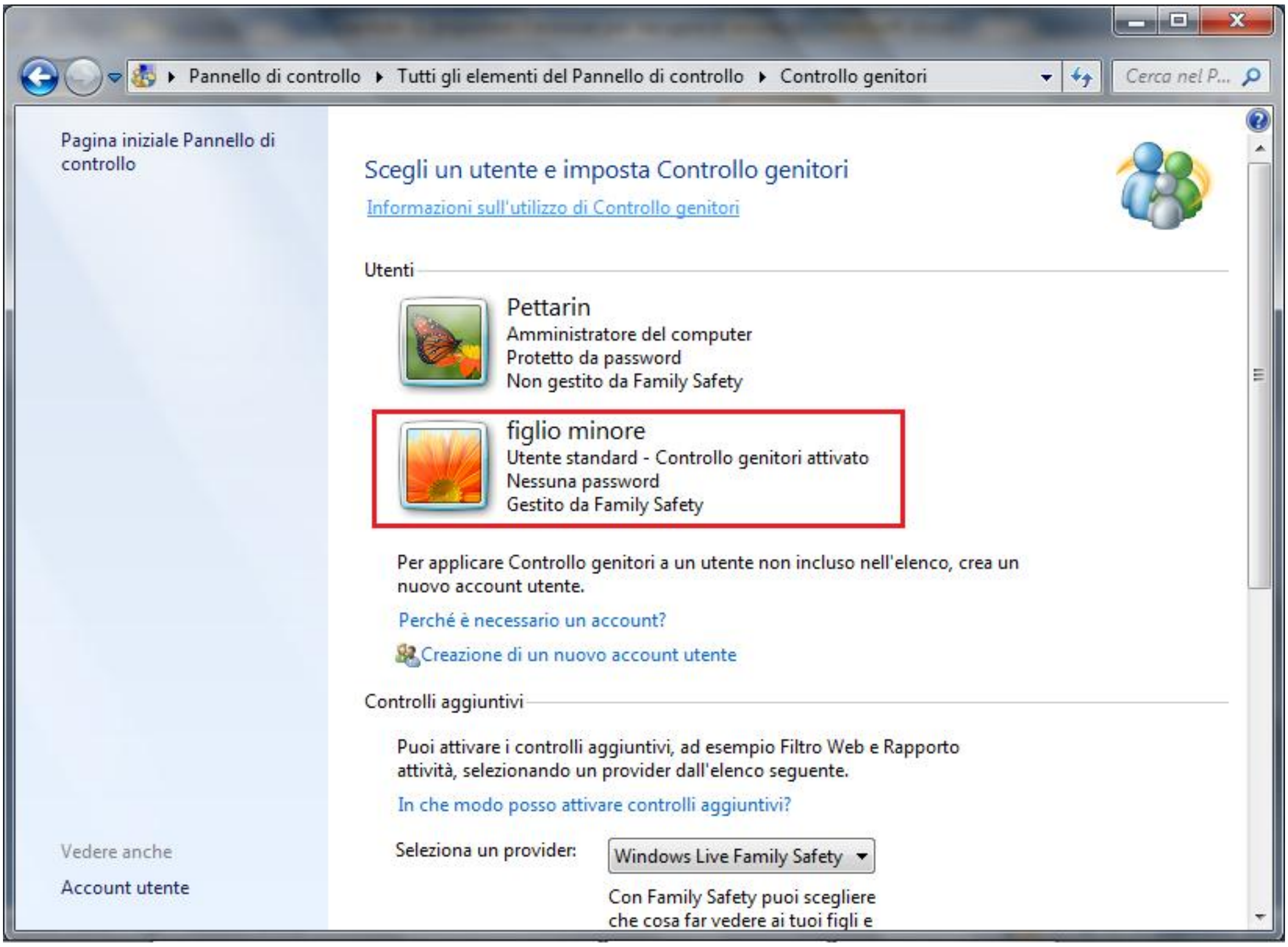
Fare clic su **Aggiungi**. Per rimuovere un sito web da un'area di sicurezza, la procedura è simile. è sufficiente fare clic su **Rimuovi**.

Controllo genitori

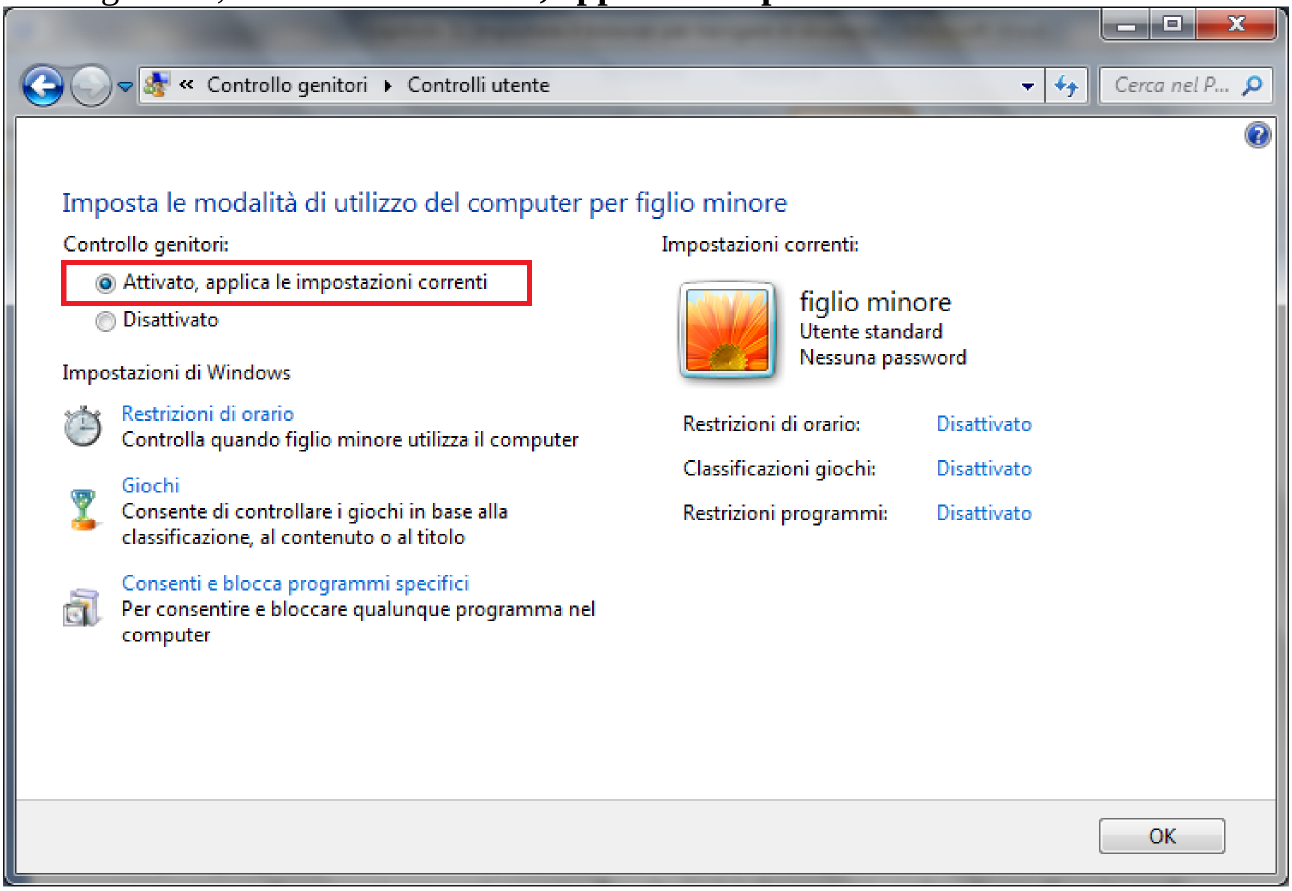
Con Windows 7 si possono impostare delle restrizioni che limitino l'uso del computer e di internet ad alcuni utenti, ad esempio i minori.
Nel Pannello di controllo, il programma **Controllo genitori** permette di impostare il tempo di utilizzo del computer da parte di un utente e specificare i programmi e i giochi che può utilizzare.



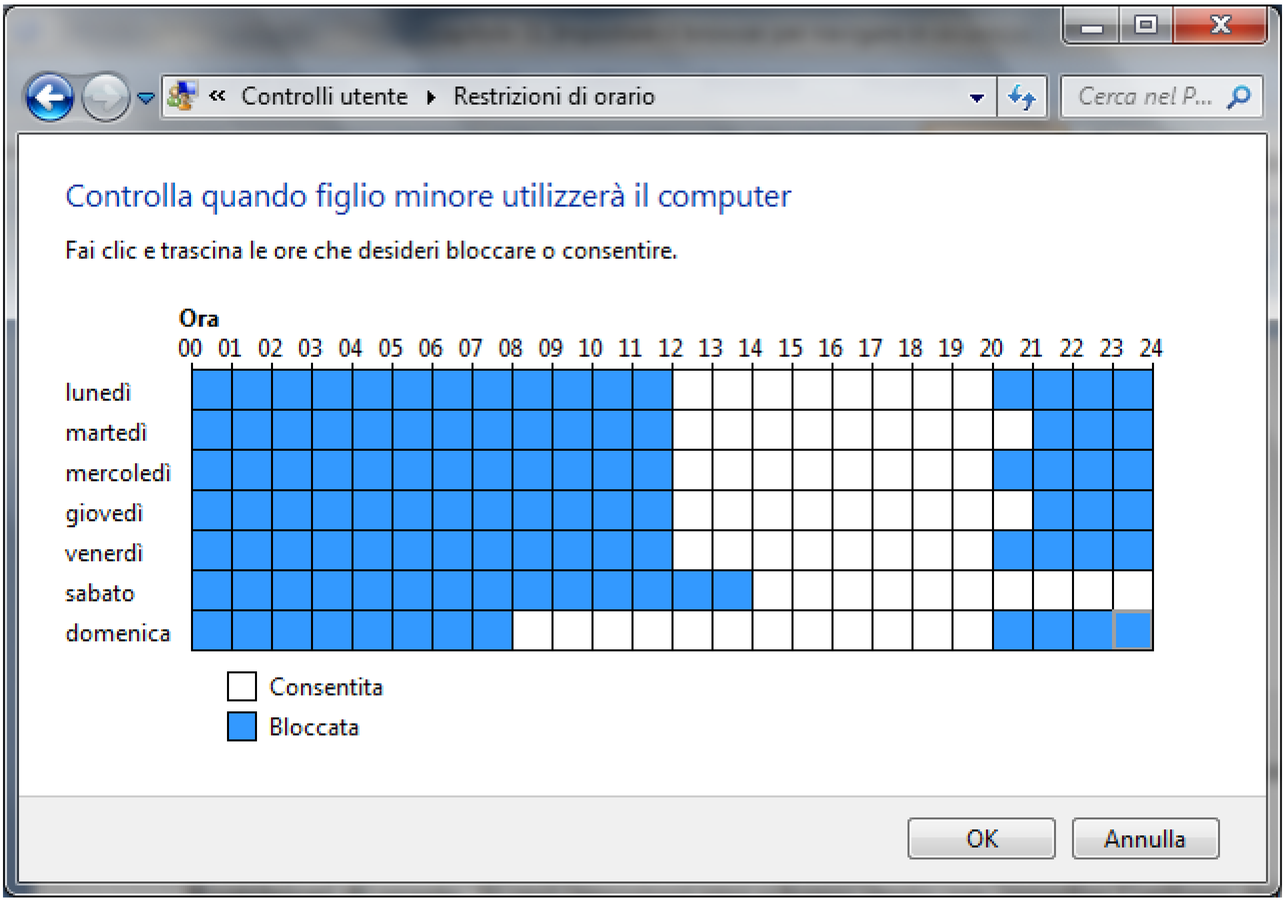
Per impostare il Controllo genitori su un utente si deve accedere come amministratore o fornire una password amministratore.



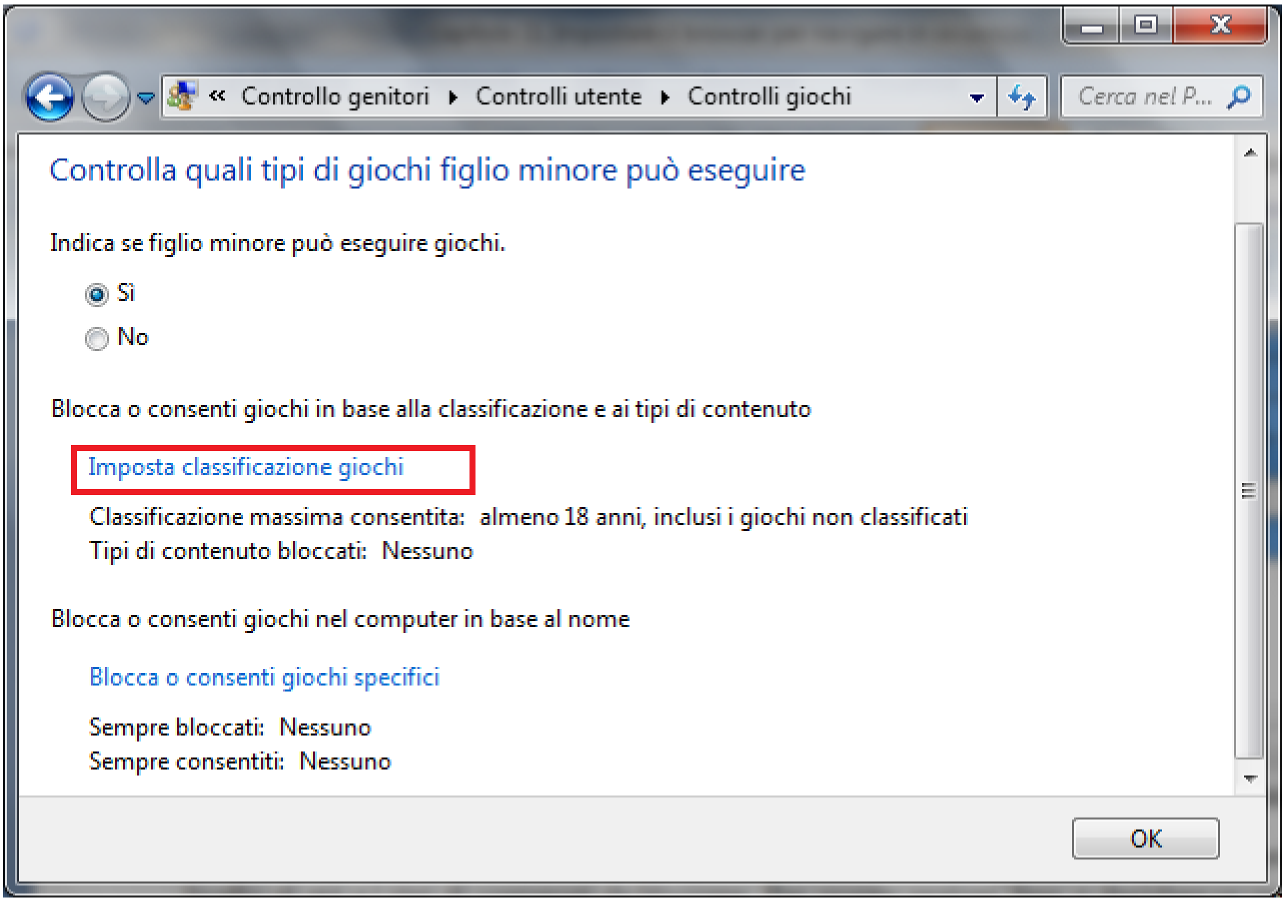
Scegliere l'account utente standard per il quale configurare Controllo genitori. Nella finestra Controllo genitori, fare clic su **Attivato, applica le impostazioni correnti**.



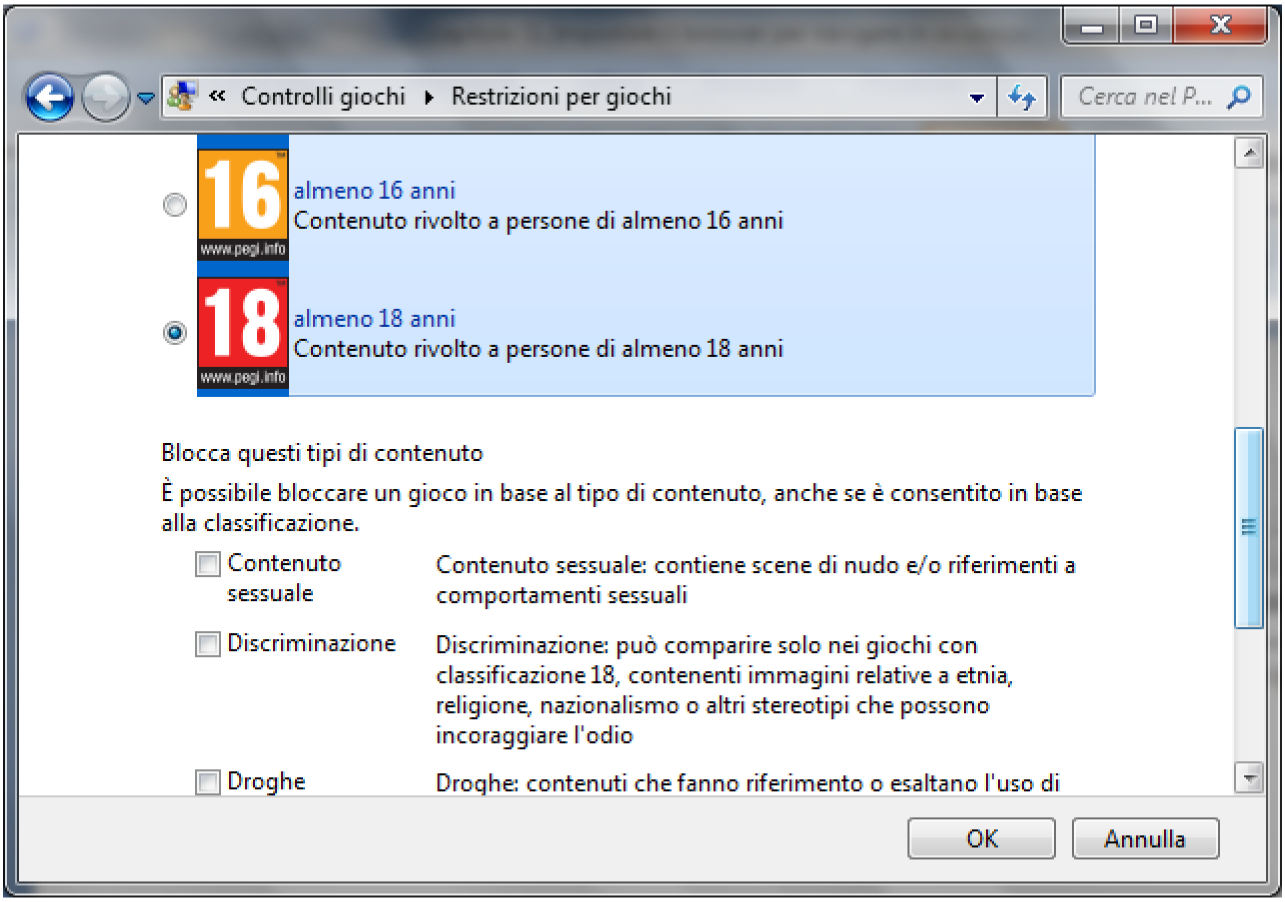
A questo punto si possono modificare le specifiche restrizioni.
Restrizioni di orario. Si può impostare uno schema orario per impedire l'utilizzo del computer nelle ore specificate, anche con orari diversi per ogni giorno della settimana.



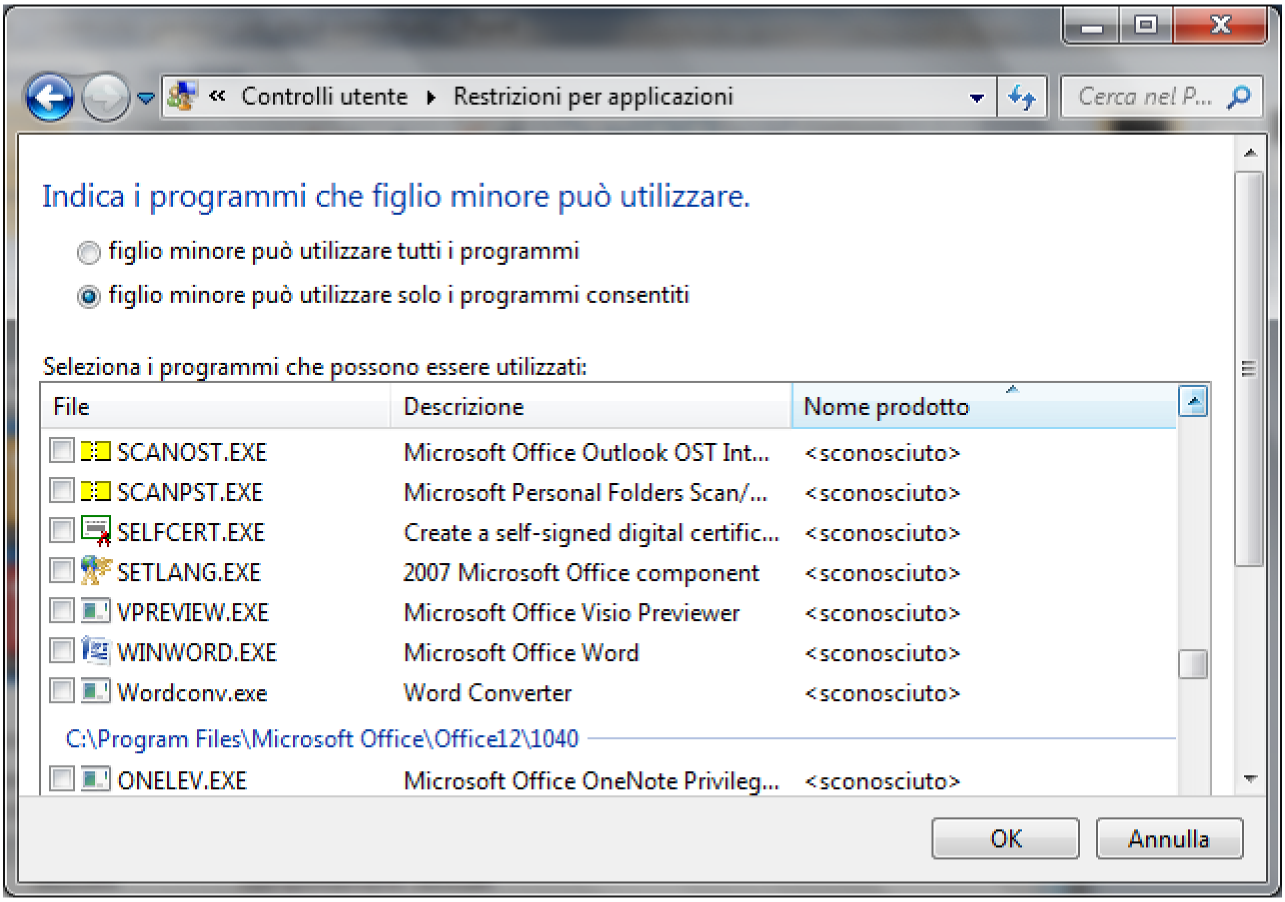
Giochi. Si può specificare quali giochi può eseguire l'utente.



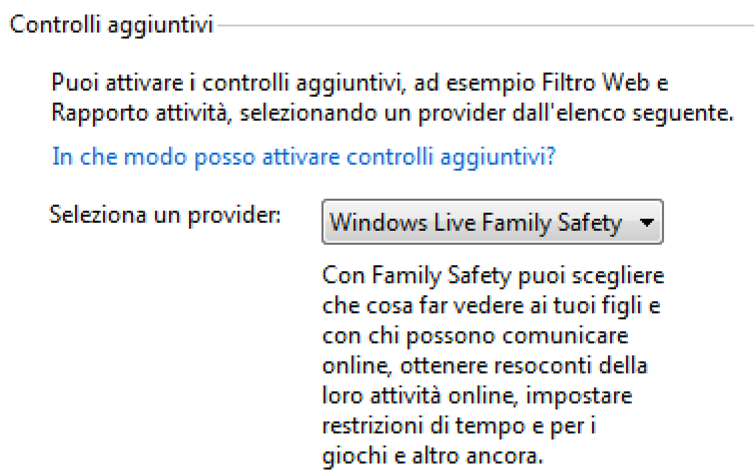
In particolare si può specificare un livello di età e i tipi di contenuti da bloccare. Per queste opzioni fare clic su **Imposta classificazione giochi**.



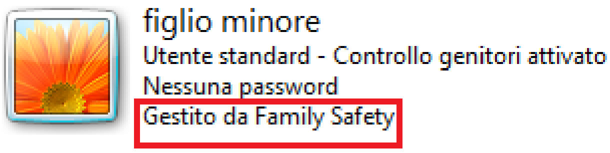
È poi possibile bloccare o consentire l'utilizzo di giochi specifici, con il comando **Blocca o consenti giochi specifici**. In modo simile è possibile
consentire o bloccare programmi specifici. Si può impedire l'utilizzo di determinati programmi con un clic sul comando **Consenti o blocca comandi specifici**.



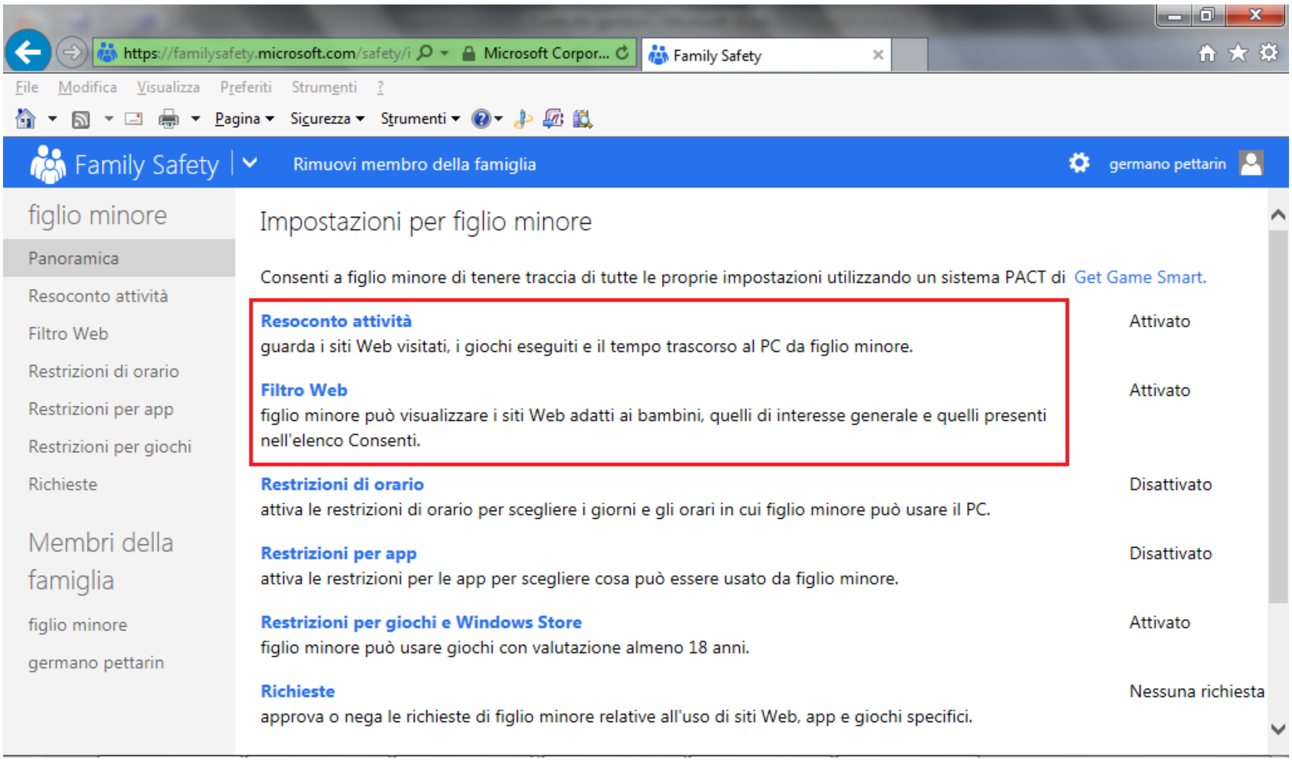
Oltre ai controlli di base inclusi in Windows, è possibile installare controlli aggiuntivi di altri provider di servizi che possono essere utilizzati in Controllo genitori, ad esempio, restrizioni per i siti Web e il resoconto attività.
Se questi controlli aggiuntivi sono già presenti nel computer appare il nome del provider nel menu del riquadro **Controlli aggiuntivi** di Controllo genitori.



Nel nostro caso è stato scelto Windows Live Family Safety. È un componente di Windows Essentials disponibile gratuitamente. Con Family Safety si può configurare il filtro Web e il resoconto attività.
Una volta selezionato il provider, tutte le funzioni del Controllo genitori, per l'utente in questione, è gestito dal sito di Family Safety.



Con un clic sull'icona dell'account si accede alla pagina di configurazione dei controlli di Family Safety.



Oltre alle opzioni già viste per Controllo genitori c'è la possibilità di filtrare i siti e di ottenere un resoconto sui siti web visitati, i giochi eseguiti e il tempo trascorso al computer.

Domande

1. I file temporanei in Windows7 per l’utente “Utente1” si trovano nella cartella
    a. Utente1\Local\Temp
    b. Utente1\AppData\Temp
    c. Utente1\AppData\Local\Temp
    d. C:\Temp
2. Tutti i cookies sono permanenti.
    a. Non esistono cookies permanenti
    b. Tutte le risposte sono errate
    c. Alcuni cookies sono permanenti, altri sono temporanei fino al termine della sessione di navigazione
    d. È vero, tutti i cookies sono permanenti
3. Le informazioni dei moduli salvate in Internet Explorer possono essere cancellate eliminando la cronologia delle esplorazioni
    a. Per Internet Explorer è esatto
    b. È falso
    c. È vero per qualunque browser
    d. È vero solo per i moduli protetti
4. Le opzioni relative al completamento automatico in IE si trovano nella omonima scheda della finestra Opzioni internet
    a. No, sono nella scheda Contenuto
    b. No, sono nella scheda Privacy
    c. No, sono nella scheda Avanzate
    d. Esatto
5. Le impostazioni “Medie” della scheda Privacy di Internet Explorer non consentono l’uso di cookies
    a. È vero
    b. È falso, consentono l’uso solo di alcuni cookies
    c. Consentono l’uso solo di cookies commerciali
    d. Consentono l’uso solo di cookies gratuiti
6. Il programma Controllo genitori permette di:
    a. Impostare il tempo di utilizzo del computer da parte di un utente
    b. Specificare i programmi che può utilizzare
    c. Specificare i giochi che può utilizzare
    d. Tutte le affermazioni sono corrette
7. La scorciatoia di tastiera in Internet Explorer per visualizzare la finestra per la cancellazione della cronologia è:
    a. CTRL+SHIFT+DEL
    b. CTRL+SHIFT+CANC
    c. CTRL+SHIFT+INS
    d. CTRL+SHIFT+ALT

Capitolo 12

Reti sociali (Social network)

Comunità virtuali in rete

Con comunità virtuale si intende un gruppo di persone riunite via Internet per valori o interessi comuni. Ad esempio, una passione, un divertimento o un mestiere o semplicemente per cercare nuove conoscenze.

Quindi in una comunità virtuale ci si incontra, si scambiano due chiacchiere (chat) o ci si vede (archivio foto degli iscritti o video chat), si leggono le ultime notizie (news), si partecipa a dibattiti e conferenze (forum e bacheca), si gioca tutti insieme (giochi on-line e concorsi), ecc.

I siti che ospitano comunità virtuali cercano di mettere a disposizione dei propri iscritti quanti più strumenti gratuiti possibili per comunicare: permettono di creare le proprie pagine personali, danno la possibilità di inviare messaggi gratuiti, hard disk virtuali on-line e quant'altro necessario per attirare l'attenzione e l'interesse.

Tra le comunità virtuali più note ci sono i **Social Network**.

I Social Network possono essere considerati come il passo successivo ai blog per esprimere la propria identità digitale nella rete: comunicare e condividere la propria vita, con persone dello stesso luogo o con persone da altre parti del mondo.

Lo scopo dichiarato di un social network è quello di mettere persone in contatto e far nascere relazioni: offrono la possibilità di creare una propria pagina web, con una struttura predefinita, dove inserire un profilo personale.

In questa pagina si può raccontare qualcosa di proprio, avere uno spazio gratuito per pubblicare link, immagini, musica video e utilizzare tutte le modalità comunicative della rete (forum, chat, inserimento di testi ed immagini, condivisione di foto/video, e-mail, Instant Messaging, ecc.) in un unico ambiente.

È possibile ricercare persone specificando dei criteri e ci sono comunità o sottogruppi basati su particolari interessi comuni.

Per iscriversi a un social network si compila un apposito modulo di adesione disponibile nel sito: oltre a fornire i propri dati personali “standard” (nome, cognome, età, residenza, ecc.), a volte, si deve rispondere a delle domande predisposte per creare il profilo del nuovo iscritto.

Una volta tracciato il profilo, si crea automaticamente la pagina web: a questo punto si è presenti nel social network. Le pagine degli utenti sono tutte basate sulla stessa struttura, in pratica sono tutte uguali. Cambiano solo le informazioni contenute, che sono quelle dichiarate nel profilo.

Nei social network è esaltata una delle caratteristiche chiave del Web 2.0 cioè la partecipazione, l’interesse attivo dei membri a trovare amici con cui condividere esperienze, incrementare le opportunità lavorative e professionali.

Facebook, è il leader fra i social network.

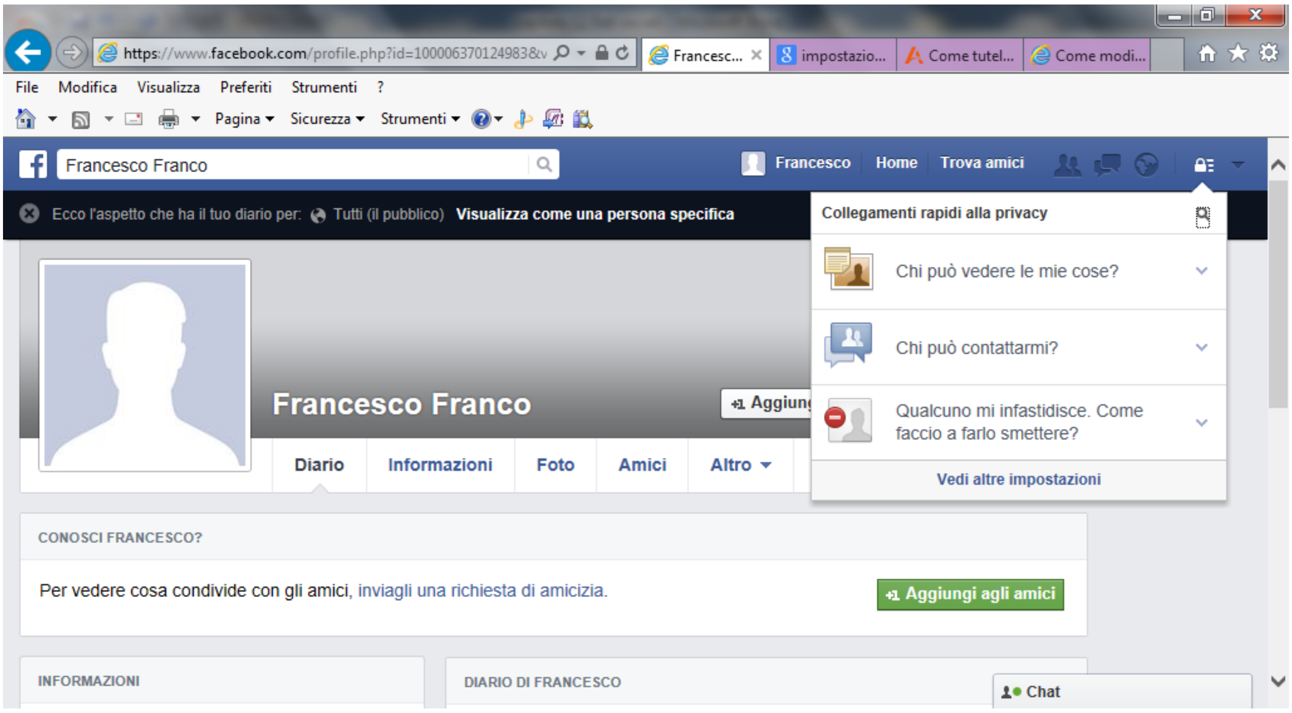
Importanza di non divulgare informazioni riservate nelle reti sociali.

Lo scopo dichiarato di un social network, mettere in comunicazione persone che non si conoscono e che desiderano iniziare nuove relazioni di amicizia, è sicuramente utile ed interessante: permette di stare in una "piazza" virtuale dove incontrarsi, conoscersi, condividere interessi, darsi appuntamenti.
Chiaramente chi gestisce un social network non è un filantropo, non lo fa solo per il bene degli utenti.
Qual è il guadagno per chi costruisce un sito di tipo Social network?
Fondamentalmente sono gli introiti pubblicitari. Se il social network ha molti iscritti e molti visitatori significa che è molto visibile in rete. La grande visibilità di un sito attira i pubblicitari che sono disposti a pagare per inserire messaggi pubblicitari nelle pagine web. Inoltre i gestori di questi siti dichiarano tranquillamente che le informazioni personali possono essere utilizzate per far arrivare messaggi pubblicitari o promozioni mirate agli interessi specificati.
Se lo scopo di un social network è positivo, è l'uso che se ne può fare che può essere pericoloso per gli iscritti. Bisogna fare molta attenzione alle informazioni che divulghiamo tramite i social network.
A questo proposito riportiamo uno stralcio di una pubblicazione del dicembre 2007 sui social network e sulla pubblicazione delle informazioni on line, da parte del CERT-Ministero della Difesa: Il CERT-Difesa è un team creato presso lo Stato Maggiore Difesa per la "Sicurezza Informatica e delle Comunicazioni". Il suo fine istituzionale è fornire informazione a scopo preventivo nel campo della sicurezza informatica.
"ATTENZIONE AI SOCIAL NETWORK SITES: La popolarità dei "social network sites" continua ad aumentare, specialmente tra i teenager e i giovani in genere. La natura di questi siti introduce però seri rischi legati alla sicurezza: per questo è raccomandabile l'utilizzo di opportune precauzioni ed effettuare opera di informazione e prevenzione per le persone meno esperte.
I social network sites si basano sullo scambio di informazioni tra i partecipanti, così incoraggiano gli utenti a mettere a disposizione una certa quantità di informazioni personali. La particolare tipologia di questi siti, il desiderio di incrementare le proprie conoscenze, il falso senso di sicurezza ingenerato dalla rete, sono i fattori che spingono gli utenti a fornire una notevole mole di informazioni personali (e immagini), non tenendo conto che queste possono cadere in mano a malintenzionati.
Fate attenzione a quello che pubblicate. In passato, era difficile trovare informazioni ulteriori a quelle relative al proprio numero di telefono o indirizzo. Oggi un sempre maggior numero di informazioni private sono disponibili on line, specialmente perché le persone creano pagine web personali con informazioni private. Nel decidere quante informazioni si vuole rivelare bisogna riflettere sul fatto che si stanno trasmettendo al mondo intero. Fornire il proprio indirizzo e mail, può aumentare il numero di spam (messaggi pubblicitari indesiderati) che si riceve.
Si consiglia di limitare per quanto possibile la quantità di informazioni personali inserite in questi siti, in particolar modo: il proprio indirizzo, informazioni circa la propria vita e le proprie abitudini. Si deve sempre tenere presente che internet è una risorsa pubblica e che chiunque può aver accesso ai dati pubblicati.

Inoltre non si deve fidarsi troppo degli estranei. Internet rende possibile poter mascherare la propria identità e le proprie motivazioni; quindi è meglio ridurre per quanto possibile il numero dei corrispondenti che ci possono contattare”.
Quindi prima di pubblicare qualcosa on line, si deve pensare al valore che hanno queste informazioni e considerare le implicazioni che possono avere quando sono disponibili al pubblico. È altrettanto importante proteggere i dati dei clienti della propria azienda e le informazioni finanziarie o produttive di essa per evitare frodi nei confronti di questi soggetti.

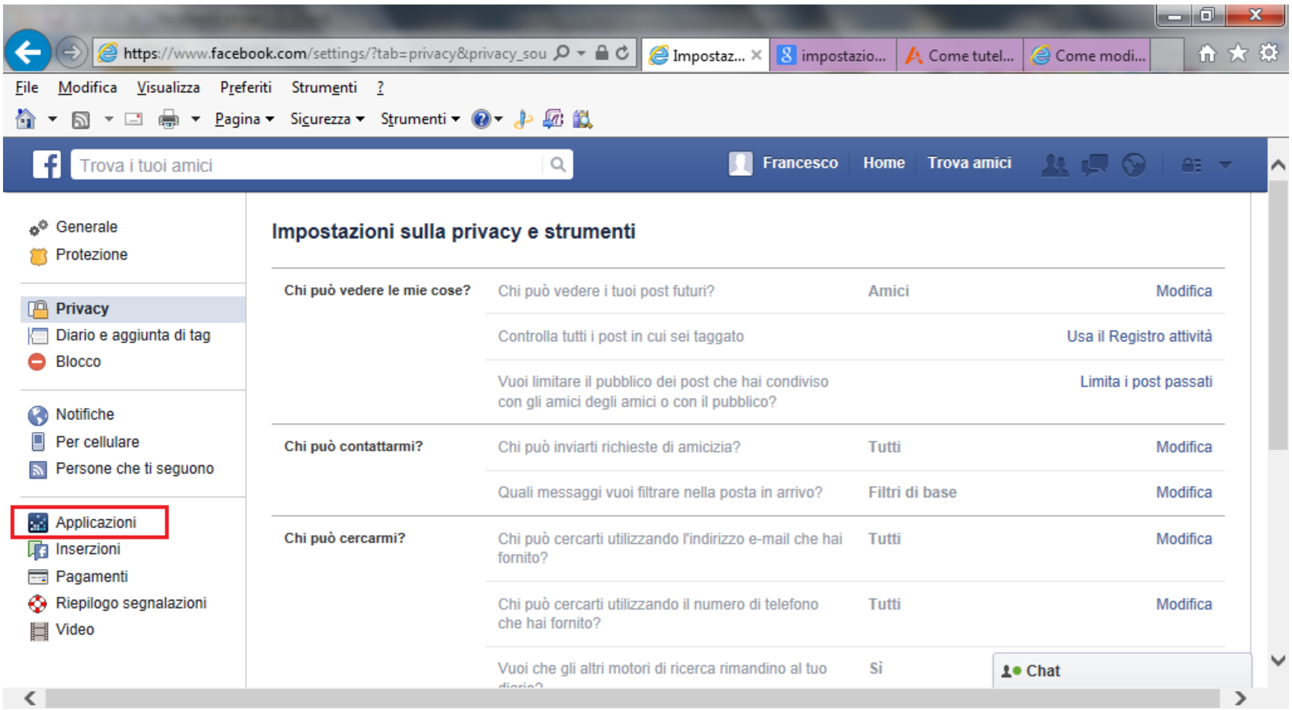
Impostazioni per la privacy in un social network

Come esempio, vediamo come tutelare la privacy dei dati personali in Facebook, in modo che degli sconosciuti non possano conoscere la città di residenza, la data di nascita, i nomi degli amici, ecc.
Nella pagina principale dell’account di Facebook, in alto a destra c’è icona con un lucchetto. Cliccando sopra di essa comparirà un menù a tendina dal quale è possibile modificare rapidamente le principali impostazioni sulla privacy.

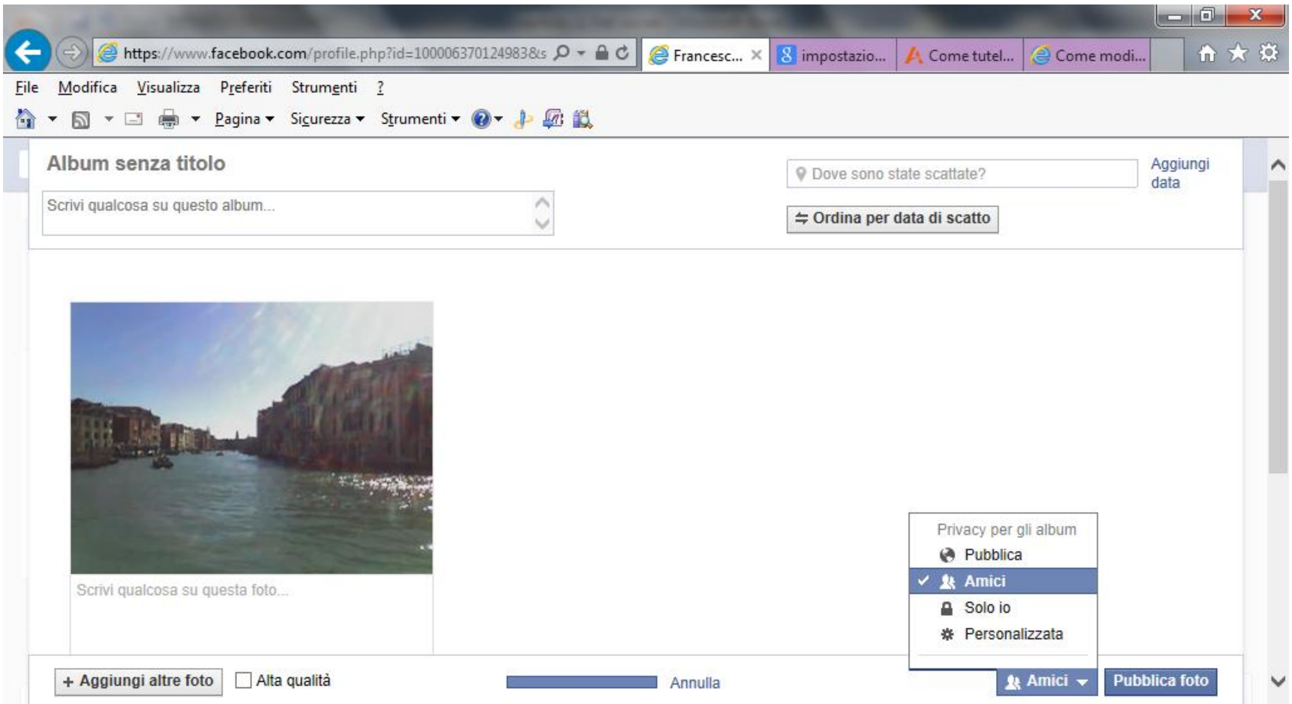


Con la voce “**Chi può vedere le mie cose”** si può configurare la visibilità dei post futuri: decidere se sono visualizzati pubblicamente, solo dagli amici, solo dall’utente stesso, solo dagli amici di amici, ecc.
Con la voce “**Chi può contattarmi”** si imposta la possibilità per altre persone di contattare o inviare richieste di amicizia. Attraverso dei filtri si potranno accettare solo i messaggi degli amici e quelli provenienti dall’elenco delle persone che si potrebbe conoscere: ad esempio, gli amici in comune. Non si riceveranno messaggi considerati spam o non sicuri inviati dalle persone che sconosciute.
L’ultima voce “**Qualcuno mi infastidisce. Come faccio a farlo smettere?”** permette di bloccare una persona (tramite nome o indirizzo email) impedendole di mandare messaggi o di interagire.

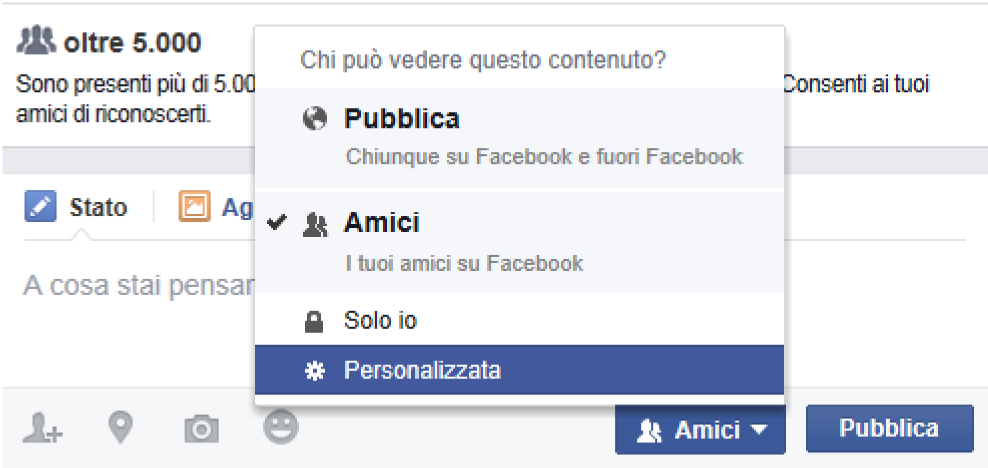
Con la voce “**Vedi altre impostazioni”** si accede alla pagina completa relativa alla privacy per l’account di Facebook. In particolare si può verificare quali applicazioni possono accedere ai dati, con la voce **Applicazioni**.



Appariranno le applicazioni alle quali abbiamo quindi concesso di accedere ad informazioni, foto, post e quant'altro del profilo.
Quanto abbiamo trattato fino ad ora riguarda le impostazioni generali. In particolare, si possono impostare limitazioni anche sui singoli elementi del profilo. Ad esempio, quando si inserisce una foto si può scegliere la relativa impostazione per la privacy dell’immagine.



Lo stesso discorso vale per i post, i video, ecc.



Rischi potenziali nell'uso delle reti sociali

Che rischi si possono incontrare con i social network? Che, come spesso accade in Internet, si deve stare attenti a cosa si fa.

I gestori di questi siti cercano di tutelarsi il più possibile da un uso non corretto della risorsa che mettono a disposizione. Spesso nelle note di utilizzo gli amministratori specificano che per accedere al servizio si deve essere maggiorenni, anche se ammettono che l'accesso dei minori ai servizi forniti dal sito non può essere in alcun modo controllato.

Inoltre il sito si deve usare in conformità alle leggi del paese dell'utente. In particolare non si può insultare, fare dichiarazioni oscene e mettere sul sito materiale pornografico o che offenda la dignità umana. Non si deve fuorviare, insultare o perseguitare altri utenti. Il fenomeno del **cyberbullismo**, l'utilizzo di internet per attaccare ripetutamente un individuo in modo sistematico, è sempre più presente in rete. Le vittime possono vedere la propria reputazione danneggiata in una comunità molto ampia, anche perché i contenuti, una volta pubblicati, possono riapparire a più riprese in luoghi diversi. Le attività online hanno spesso conseguenze anche nella vita reale.

Anche l'**adescamento**, o **grooming** (tecnica psicologica utilizzata per l'adescamento di minori in rete per ottenere comportamenti inappropriati) è un fenomeno frequente in rete. È un reato, recentemente introdotto nel nostro codice penale: si riferisce al compimento di qualsiasi atto volto a carpire la fiducia di un minore di età inferiore a sedici anni per scopi sessuali, attraverso artifici, lusinghe o minacce posti in essere mediante internet o altre reti o mezzi di comunicazione. Il reato si configura anche se l'incontro con il minore non avviene: non è necessario, infatti, che l'adescamento vada a buon fine, ma è sufficiente il tentativo, da parte di un adulto, di conquistare la fiducia di un bambino o di un adolescente per fini sessuali.

I gestori del sito si riservano il diritto di accedere a tutto il materiale pubblicato sul sito e cancellare il materiale quando necessario per la moderazione: inoltre può comunicare alle autorità competenti tutte le attività e/o materiali illegali pubblicati sul sito.

Chiaramente i gestori fanno quello che possono: è ovvio che non possono controllare tutto quello che viene pubblicato (soprattutto se il social network assume grandi dimensioni). Inoltre non possono fare nulla se l'utente dichiara nell'iscrizione dei dati falsi e non può sapere quali sono le reali intenzioni di chi accede al loro servizio. Si parla di **false identità** o **fake**, usate proprio per tentativi di adescamento e cyberbullismo. Secondo la Cassazione chi crea una falsa identità sul web commette un reato, in quanto "si lede la fede pubblica degli utenti che credono di parlare con una persona diversa quella che si è nella quotidianità".

In conclusione, con i social network, e genericamente con internet, si deve lasciarsi guidare dal buon senso.
Si deve fare anche attenzione quando si pubblica materiale che riguarda altri. Ad esempio, per filmare una persona e pubblicare il file in rete, sarebbe necessario avere il consenso del soggetto interessato. Questo consenso può essere gestito in modi diversi: il soggetto può revocare il consenso dato, oppure essere d’accordo di apparire in alcuni siti e non in altri, ecc.
In realtà si deve valutare caso per caso. Ad esempio nel caso di personaggi pubblici (un cantante, un uomo politico, un atleta, ecc.) non è richiesto il consenso: basta che non venga leso l’onore e la reputazione della persona.
Oppure, nel caso di persone comuni, non serve il consenso se sono in un luogo pubblico e il soggetto fa parte della situazione o del luogo (ad esempio un filmato panoramico di un parco), cioè la persona non è isolata dal contesto.

Domande

1. Cosa sarebbe meglio non pubblicare in un social network?
    a. Informazioni personali riservate
    b. Dati dei clienti della propria azienda
    c. Informazioni finanziarie o produttive riservate della propria azienda
    d. Tutte le affermazioni sono corrette
2. Che rischi si possono incontrare con i social network?
    a. Adescamento
    b. Cyber bullismo
    c. False identità
    d. Tutte le risposte sono corrette
3. Le opzioni di privacy nei Social Network sono inutili, i dati pubblicati sono accessibili da chiunque
    a. È falso
    b. È vero solo in Facebook
    c. È vero per ogni Social Network
    d. È vero solo per le immagini
4. In FaceBook è possibile segnalare una persona per stalking
    a. Solo se è maschio
    b. Solo se è maggiorenne
    c. Non è possibile
    d. Si, è possibile
5. Come si definisce una persona che molesta con offese e minacce in rete?
    a. Cyberbullo
    b. Hacker
    c. Cracker
    d. Black Hat
6. Una caratteristica del cyberbullismo è:
    a. non ha limiti di orario
    b. anonimato del molestatore
    c. senso di impunità
    d. tutte le risposte sono corrette
7. Per le vittima è generalmente difficile identificare il Cyberbullo che la sta importunando se questi vuol restare anonimo
    a. È falso
    b. È vero
    c. Solo nel caso di IM
    d. Solo nel caso di E mail

Capitolo 13

Capitolo 13 Posta elettronica in sicurezza

La posta elettronica

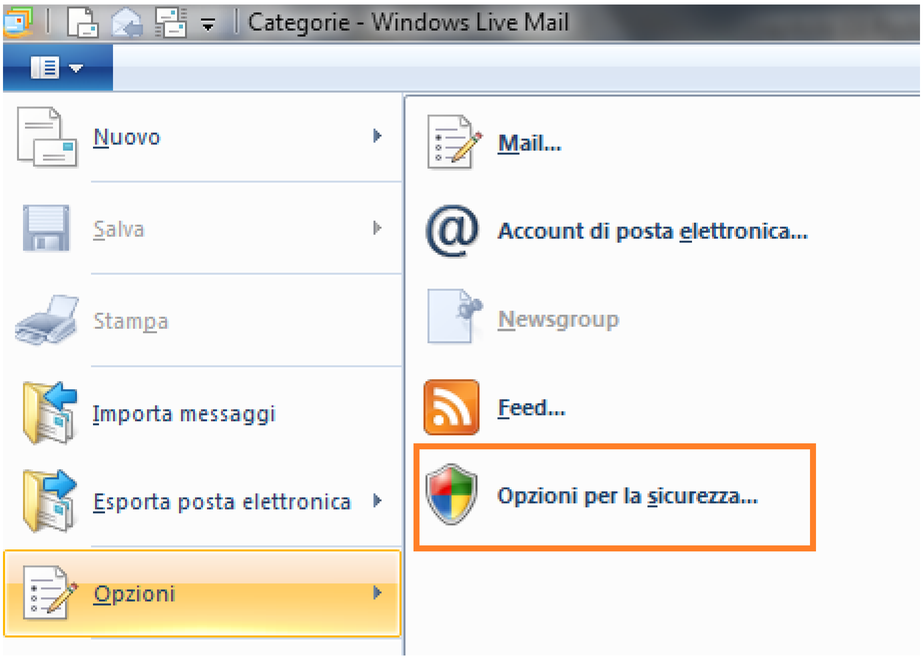
La posta elettronica o e-mail ovvero electronic-mail è uno dei più importanti servizi offerti in Internet.
La filosofia operativa della posta elettronica ricalca quella della posta tradizionale: esiste un messaggio da spedire a un destinatario da parte di un mittente ed entrambi hanno un indirizzo che li identifica.
Ma rispetto al servizio di posta tradizionale l'e-mail offre, come molti vantaggi:

- un messaggio può essere spedito contemporaneamente a più destinatari;
- il costo è quello del collegamento ad internet;
- si possono allegare al messaggio altri documenti, immagini, suoni, programmi, ecc;
- se il messaggio, per qualche motivo, non può giungere a destinazione, si ha una immediata notifica del mancato recapito;
- si può costruire una rubrica elettronica di destinatari.

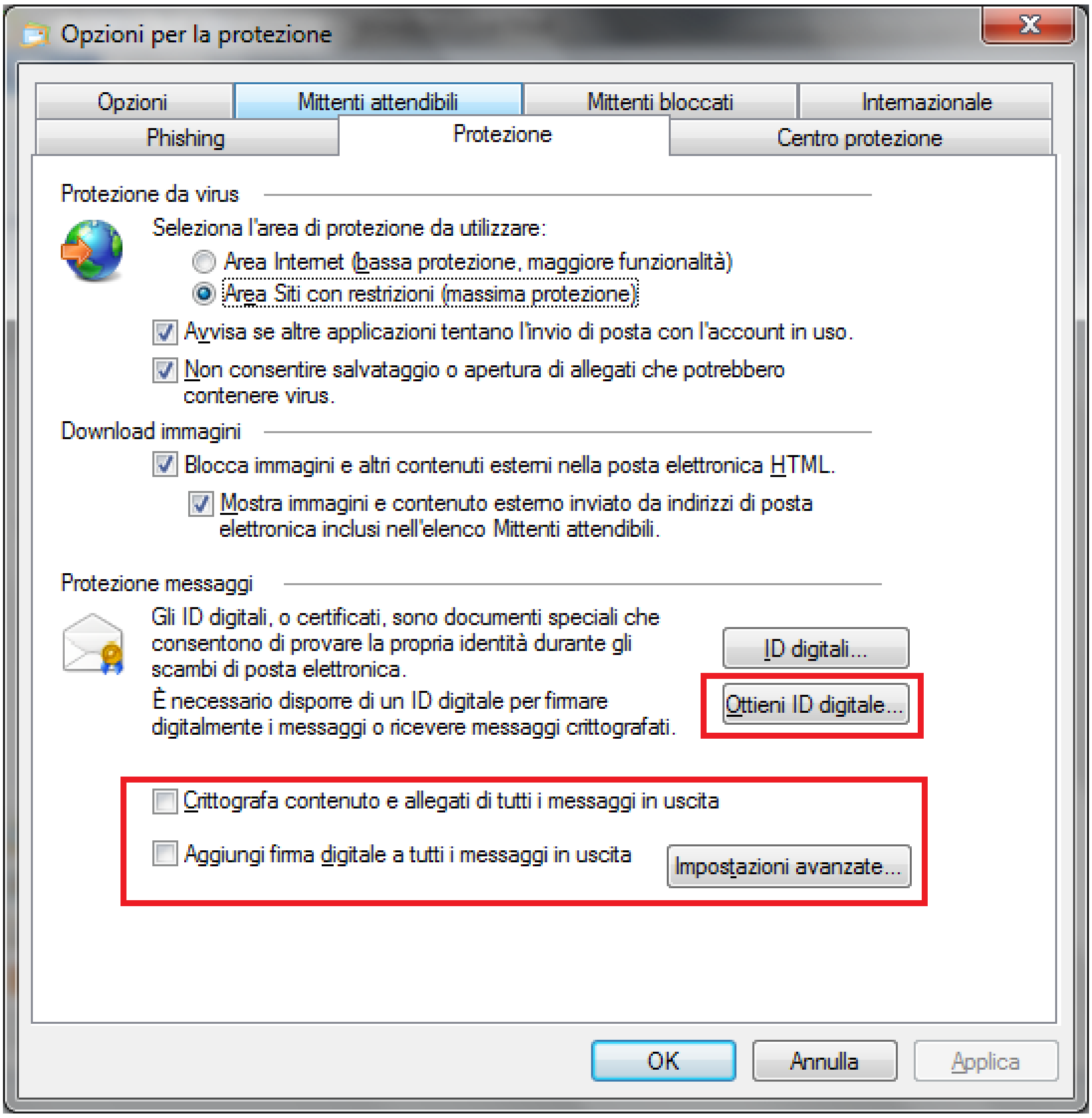
Per poter utilizzare la posta elettronica sono necessari un computer, un modem, ed un accesso ad internet. Può essere necessario aver installato nel computer un programma di gestione della posta elettronica (*posta off line*), ma è possibile utilizzare la posta elettronica anche via web con il servizio di *posta on line*.
Un vantaggio nell'utilizzare i programmi di gestione della posta off line sta nella possibilità di poter mantenere e consultare tutta la posta che abbiamo ricevuto (posta in arrivo) o spedito (posta inviata) senza collegarsi ad internet.
Nel capitolo useremo il servizio di posta off line Windows Live Mail.

Aggiungere una firma digitale o crittografare un messaggio

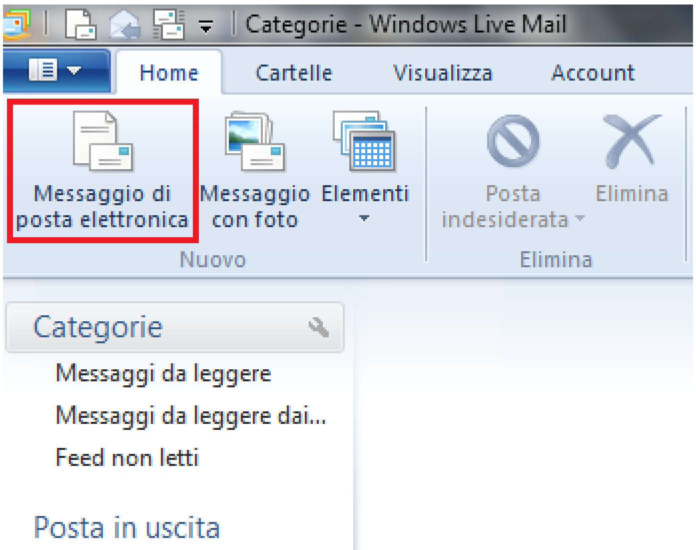
La posta elettronica è normalmente un mezzo di comunicazione non sicuro dato che i messaggi vengono inviati in chiaro: se viene intercettato può essere letto da chiunque.
Per rendere l'invio di un messaggio sicuro, se all'account di posta elettronica è collegato un **ID digitale**, si può aggiungere ai messaggi di Windows Live Mail una firma digitale per confermare la propria identità, oppure **crittografare** i messaggi, in modo che solo il legittimo destinatario, in possesso di una chiave di decodifica, sia in grado di leggerlo.
Un ID digitale consente di verificare l'identità del mittente e del destinatario di un messaggio e-mail e può impedirne la manomissione. Gli ID digitali consentono di proteggere i messaggi aggiungendo un codice univoco denominato **firma digitale** al messaggio. La firma assicura ai destinatari dei messaggi e-mail che questi ultimi provengano effettivamente dal mittente indicato.
Per ottenere un ID Digitale Scegliere la voce **Opzioni per la sicurezza** nel menu delle **Opzioni**.



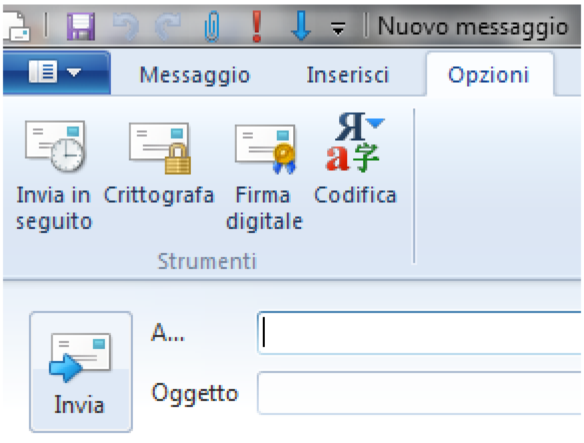
Nella scheda **Protezione**, fare clic su **Ottieni ID digitale**.



Appare una pagina web con le Autorità di certificazione. Si deve selezionarne una e seguire le istruzioni: l'autorità invierà per posta elettronica l'ID digitale e le istruzioni di configurazione.
A questo punto è possibile aggiungere la firma digitale a un messaggio o crittografarlo. Notiamo che nella scheda Protezione si possono impostare queste modalità in automatico.
Con un clic su **Messaggio di posta elettronica** creare un messaggio nuovo.



Nella barra multifunzione selezionare la scheda **Opzioni**.

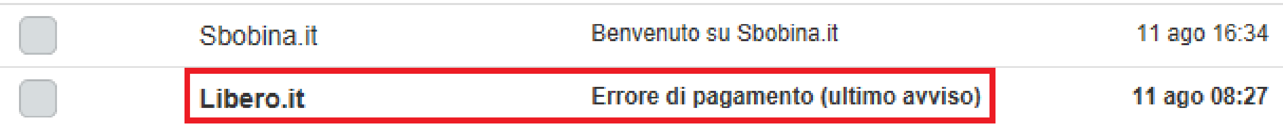


Con **Firma digitale** e **Codifica** si inserisce rispettivamente la firma digitale e la crittografazione del messaggio.
Quando si inviamo i messaggi con la firma digitale è presente l'icona di una coccarda. I messaggi crittografati hanno l'icona di un lucchetto.

Spam e altri tipi di e mail indesiderate

La posta elettronica è uno strumento utile e comodo e molto spesso può sostituire la posta originale. Chiaramente ci possono essere degli usi non corretti. Il più tipico esempio è lo **Spam**, ovvero la ricezione di messaggi pubblicitari, via e mail, non richiesti. È meglio non rispondere a questo tipo di messaggi, altrimenti si confermerebbe l'indirizzo e mail in uso e lo spammer aumenterebbe l'invio di messaggi.

Un altro esempio, come abbiamo già visto e il **Pishing**. Il phishing è una strategia volta a carpire con l'inganno le informazioni personali o finanziarie degli utenti della rete attraverso un messaggio di posta elettronica o un sito Web. Una comune frode tramite il pishing online si basa su un messaggio di posta elettronica simile a un avviso ufficiale inviato da un'origine attendibile, ad esempio una banca, una società emittente di carte di credito o un commerciante di chiara reputazione. I destinatari del messaggio di posta elettronica vengono indirizzati a un sito web fraudolento, in cui viene richiesto di fornire informazioni personali, ad esempio un numero di conto o una password. Queste informazioni vengono quindi utilizzate per appropriarsi dell'identità altrui. In figura un esempio di pishing.



Il comportamento da tenere con questo tipo di messaggio è quello di cancellarli subito senza nemmeno aprirli.
Come ultima cosa, si deve far particolare attenzione agli allegati di posta elettronica dato che possono contenere delle macro maligne o altro tipo di software infetto. Si consiglia, prima di aprire un allegato, di fare una scansione con un software antivirus.

Sicurezza con la messaggistica Istantanea (IM)

La messaggistica istantanea, o IM, è un mezzo per comunicare istantaneamente attraverso messaggi di testo, e in molti casi anche audio e video, con i propri amici, cioè con chi è stato accettato come membro nel servizio, in modo diretto e immediato.
Spesso con l'IM si può vedere la presenza degli amici, cioè se sono effettivamente in linea nello stesso momento. Esempi di programmi di istant messaging sono Skype, Messenger, AIM.
Per utilizzare l'IM, è necessario installare sul computer uno tra i vari programmi gratuiti e scegliere un nome identificativo da visualizzare sullo schermo. Poi si deve ottenere i nomi identificativi di amici e conoscenti e aggiungerli all'elenco dei contatti del programma, il quale funziona né più né meno come una normale rubrica di indirizzi di e-mail o di numeri di telefono.
Per interagire con un amico, è sufficiente fare clic sul suo identificativo nell'elenco, scrivere il messaggio e inviarlo. Il messaggio viene visualizzato sullo schermo dell'amico con una velocità maggiore di quella richiesta da un'e-mail per viaggiare a destinazione in Internet. A questo punto può avere luogo una conversazione interattiva. Di fatto, la maggior parte dei programmi di messaggistica istantanea consente anche di dialogare faccia a faccia con l'ausilio di webcam.
Come la posta elettronica, anche la messaggistica istantanea comporta il rischio di ricevere sul proprio computer malware che possono comprometterne la sicurezza. Alcuni pericoli possono essere:
Spamming, messaggi istantanei indesiderati pubblicitari. A volte, i messaggi che vengono visualizzati sembrano provenire dalla propria banca o da un concorso a premi, mentre in realtà i mittenti sono persone malintenzionate che stanno tentando carpire informazioni di carattere personale e finanziario (pishing).

Worm, virus, trojan. Analogamente alle e-mail, i programmi nocivi possono infettare anche la messaggistica istantanea e creare delle backdoors. Se questo accade, i contatti riceveranno messaggi istantanei infetti.
Per la sicurezza con l’IM, non esistono rimedi validi contro ogni evenienza.
In generale, è preferibile **bloccare i mittenti indesiderati o sconosciuti**, regolando le impostazioni della messaggistica istantanea in modo da accettare messaggi sono da coloro che sono presenti nell’elenco dei contatti.
È meglio **non fornire informazioni personali** e non rendere noto on-line il proprio identificativo di messaggistica istantanea. È consigliabile che tutti i famigliari scelgano nomi che non comprendono dettagli personali. Molti programmi di messaggistica istantanea consentono anche di creare profili. Per garantire un'ulteriore protezione della privacy, è meglio ignorare questa opzione o non includere alcuna informazione di identificazione o fotografia.
Non aprire collegamenti o allegati non richiesti. Anche se un collegamento web sembra provenire da un amico, in realtà potrebbe essere stato inviato da un worm o da un altro programma sospetto con l'obiettivo di infettare il tuo computer.
Altri consigli, simili a quelli per la posta elettronica, sono la cifratura delle informazioni e non condividere di file importanti.

Domande

1. Cosa si intende per Spam?
    a. Una tipologia di malware
    b. Una chiave di sicurezza di rete
    c. La ricezione di messaggi pubblicitari, via e mail, non richiesti
    d. Una opzione del browser
2. Quando si riceve un messaggio Spam
    a. È meglio non rispondere al messaggio per non confermare l'indirizzo e mail in uso
    b. È meglio rispondere specificando che non si vuole più ricevere messaggi di quel tipo
    c. Si deve rispondere solo se il messaggio contiene informazioni finanziarie
    d. Tutte le risposte sono errate
3. Quale dei seguenti è un rischio con la e mail?
    a. Importazione di virus tramite allegati
    b. Pishing
    c. Spam
    d. Tutte le risposte sono corrette
4. Quali cautele sono consigliabili con l'IM?
    a. Bloccare i mittenti indesiderati o sconosciuti
    b. Non rendere noto on-line il proprio identificativo di messaggistica istantanea
    c. Non condividere di file importanti
    d. Tutte le affermazioni sono corrette
5. Quale dei seguenti è un rischio con la Messaggistica Istantanea?
    a. Installazione Malware
    b. Pishing
    c. Accesso da backdoors
    d. Tutte le risposte sono corrette

Capitolo 14

Messa in sicurezza e salvataggio dei dati

Sicurezza "fisica" e sicurezza software dei dati

Per prevenire la perdita dei dati personali e/o aziendali è opportuno cautelarsi dai danni e dai furti dei dispositivi dove sono memorizzati e predisporre dei meccanismi per creare copie di sicurezza in modo periodico e sistematico.

Sicurezza fisica dei dispositivi

Per evitare il furto o lo smarrimento dei dati, prima di tutto è necessario mettere in sicurezza "fisica" i dispositivi informatici in modo da impedirne la sottrazione da parte di malintenzionati.
In generale, non si deve lasciare il dispositivo incustodito in un'area facilmente accessibile al pubblico. Di quanta sicurezza fisica si ha bisogno sul sistema dipende molto dalla situazione e/o dal budget.
Se si è un utente casalingo, probabilmente non ne serve molta. Se si tratta di un laboratorio o di una rivendita di computer, ne servirà molta di più, ma gli utenti dovranno comunque essere in grado di lavorare sulle macchine.
Se si è in un ufficio, si potrebbe o meno avere bisogno di tenere al sicuro le macchine fuori dall'orario di lavoro o quando non si è presenti. In certe società, lasciare incustodita la propria postazione è un motivo di licenziamento.
Molti case dei moderni PC includono la possibilità di essere chiusi. In genere hanno una toppa sulla parte frontale che serve per chiudere e aprire con una chiave. Queste serrature possono aiutare ad evitare che qualcuno rubi il PC, o che apra il case e manipoli o rubi i componenti.
Questa caratteristica può essere molto utile, anche se le serrature sono in genere di bassissima qualità e possono essere facilmente eluse con lo scasso.
Un modo molto utilizzato nelle rivendite di computer è l'uso di cavi di sicurezza, tra cui i più diffusi seguono lo standard Kensington Security Lock.



Sono dei cavi ultraspessi, realizzati con materiali di qualità superiore e un lucchetto a disco antimanomissione.
Un'altra possibilità è di usare il BIOS per evitare che un intruso riavvii la macchina e manipoli il sistema.
Molti BIOS di PC permettono di usare una password di avvio. Questo non offre molta sicurezza (il BIOS può essere resettato o rimosso se qualcuno può aprire il case), ma potrebbe essere un buon deterrente.
Un altro motivo per non fidarsi delle password di avvio è il problema delle password predefinite. Molti produttori di BIOS non si aspettano che la gente apra il proprio computer e stacchi le batterie se si dimentica della propria password e hanno perciò equipaggiato i BIOS con delle password predefinite che funzionano indipendentemente dalla password scelta.
È inoltre importante tenere traccia della collocazione dei dispositivi, così come dei loro dettagli, in modo da poter verificare in modo preciso eventuali mancanze.
Infine è utile controllare gli accessi ai locali nei quali i dispositivi sono collocati, in modo da poter più facilmente risalire all'autore di eventuali furti.

Importanza di avere una procedura di copie di sicurezza

A parte il furto dei dispositivi, ci possono essere altre cause che possono portare alla perdita di dati fondamentali. Ad esempio:

- danneggiamento dell'hard disk,
- danni elettrici dovuti a repentini sbalzi di tensione,
- incendio,
- allagamento,
- furto,
- sabotaggio,
- virus informatici,
- imperizia dell'utente.

È quindi importante avere una copia di sicurezza (**backup**) dei dati che permetta di ricostruirli in caso di perdita.
Fare il backup significa copiare tutti i dati del sistema su di un supporto esterno come un hard disk esterno, un hard disk in rete, una unità nastro, un CD/DVD, una chiave USB, ecc.
Il backup permette di mantenere una copia di riserva dei propri dati e programmi. In caso di perdita accidentali dei dati originali, per sbalzi di tensione, danni hardware, incidenti, furti, ecc. si ha la possibilità di ripristino della situazione esistente fino all'ultimo backup.
I dati da salvare nella copia di sicurezza sono quelli che l'utente ritiene importanti per la sua attività, le informazioni di carattere finanziario, i siti preferiti e la cronologia del browser.
La maggior parte degli utenti riesce a capire l'importanza dell'operazione di backup dei file.
Le principali ragioni per cui molti utenti non effettuano le operazioni di backup possono riassumersi in 4 punti:

- non sono al corrente della possibilità di poter fare copie di sicurezza;
- non si sono mai posti questo problema;
- non sono a conoscenza delle procedure per la realizzazione delle copie di sicurezza;
- la procedura di effettuazione di copie di sicurezza comporta dispendio di tempo e denaro.

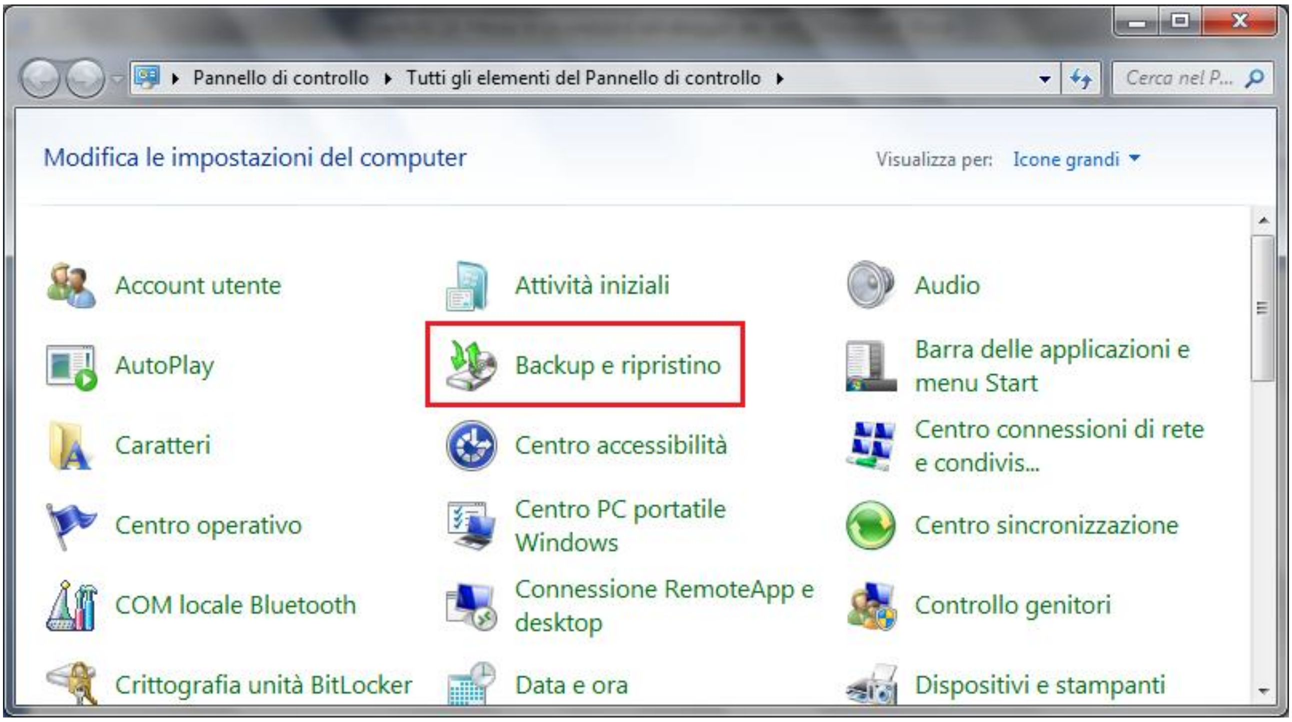
Caratteristiche di una procedura di copie di sicurezza

Per evitare di dimenticarsi di effettuare la copia di sicurezza, è opportuno impostare un programma di copia in modo che questa avvenga automaticamente a scadenze regolari in un momento in cui il computer rimane acceso ma non viene utilizzato, ad esempio di notte o fuori dall'orario di lavoro, per evitare che la copia dei dati rallenti il lavoro.
Le caratteristiche fondamentali di una procedura di backup efficiente sono:
dove conservare le copie. È il caso di conservare la copia dei dati in un luogo diverso da quello di installazione dell'elaboratore; conservare i propri file su un disco rigido interno o esterno ma costantemente collegato al computer non è una buona idea: un ladro o un incendio porterebbero a una perdita irrecuperabile. Bisogna conservare le copie in zone differenti dell'abitazione/ufficio, se possibile anche in edifici diversi. Una possibilità è utilizzare i servizi di **Cloud Storage** come DropBox.
frequenza delle copie. La frequenza dei backup è funzione della rapidità con cui cambiano i dati e dell'importanza che rivestono. Se si usa il computer sporadicamente, una o due volta alla settimana, una copia di sicurezza mensile è sufficiente. In caso di uso giornaliero, bisogna effettuare copie almeno settimanalmente. In ambito lavorativo, se si inseriscono quotidianamente dati importanti, diventa necessario effettuare quotidianamente anche i backup.
Una banca effettua dei backup delle proprie transazioni praticamente in tempo reale. Un'azienda commerciale potrebbe effettuarlo giornalmente, magari a fine giornata lavorativa, durante la notte.
Una pratica comune è quella di effettuare dei full backup settimanalmente, durante il fine settimana, e degli incremental backup o differential backup ogni sera da lunedì a venerdì. Situazioni articolate possono richiedere la supervisione di personale tecnico.
Quali dati copiare. È importante valutare quali dati devono essere oggetto di backup. Sicuramente i dati importanti per la propria attività. Non sono da dimenticare le e-mail, la rubrica, i siti preferiti, la cronologia, ecc. Oltre ai dati veri e propri è una buona idea effettuare copie di backup dei programmi in uso, così che, se necessario, sia possibile reinstallarli semplicemente.
Quali dispositivi utilizzare. Esistono numerosi dispositivi e supporti di memorizzazione, ognuno con punti di forza e debolezza. La prima cosa da chiarire con precisione è quali siano le proprie esigenze. Generalmente è una buona idea adottare dispositivi che permettano di effettuare l'intera copia su di un solo supporto per evitare la supervisione e l'intervento di un operatore per l'inserimento in successione dei vari supporti.
Il disco rigido esterno è sicuramente un dispositivo valido, in grado di offrire istantaneamente una grande capacità ed una buona velocità. Nel caso non si necessiti di molto spazio le chiavette USB sono convenienti e affidabili. Da non scordare neanche CD / DVD, ormai sempre presenti nei PC, sebbene la stabilità nel lungo periodo sia inferiore a quanto si pensi comunemente.
In ambito aziendale le cassette (tape backup) hanno ancora ampia diffusione, come i dischi rigidi, spesso integrati in dispositivi NAS.
Qualsiasi sia la scelta, bisogna prediligere sistemi che minimizzino la necessità di interventi manuali e permettano una semplice pianificazione dei backup. Inoltre è fondamentale che la copia sia conservata in un luogo sicuro e diverso da dove si trovano i dati originali.

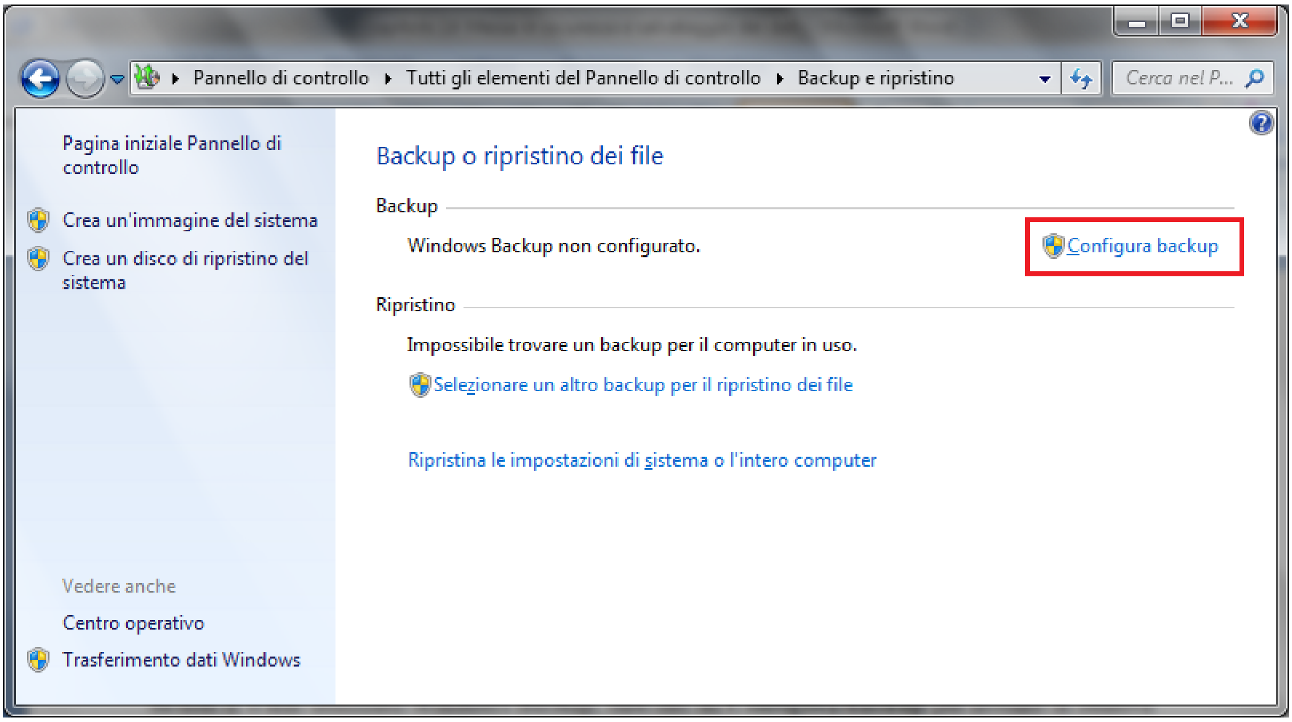
Come ultima cosa è meglio eseguire un ripristino di prova per verificare che le copie dei file siano state eseguite correttamente. In questo modo si individueranno eventuali problemi nell'hardware non rilevati con le verifiche software.

Effettuare una copia di sicurezza con Windows 7 backup

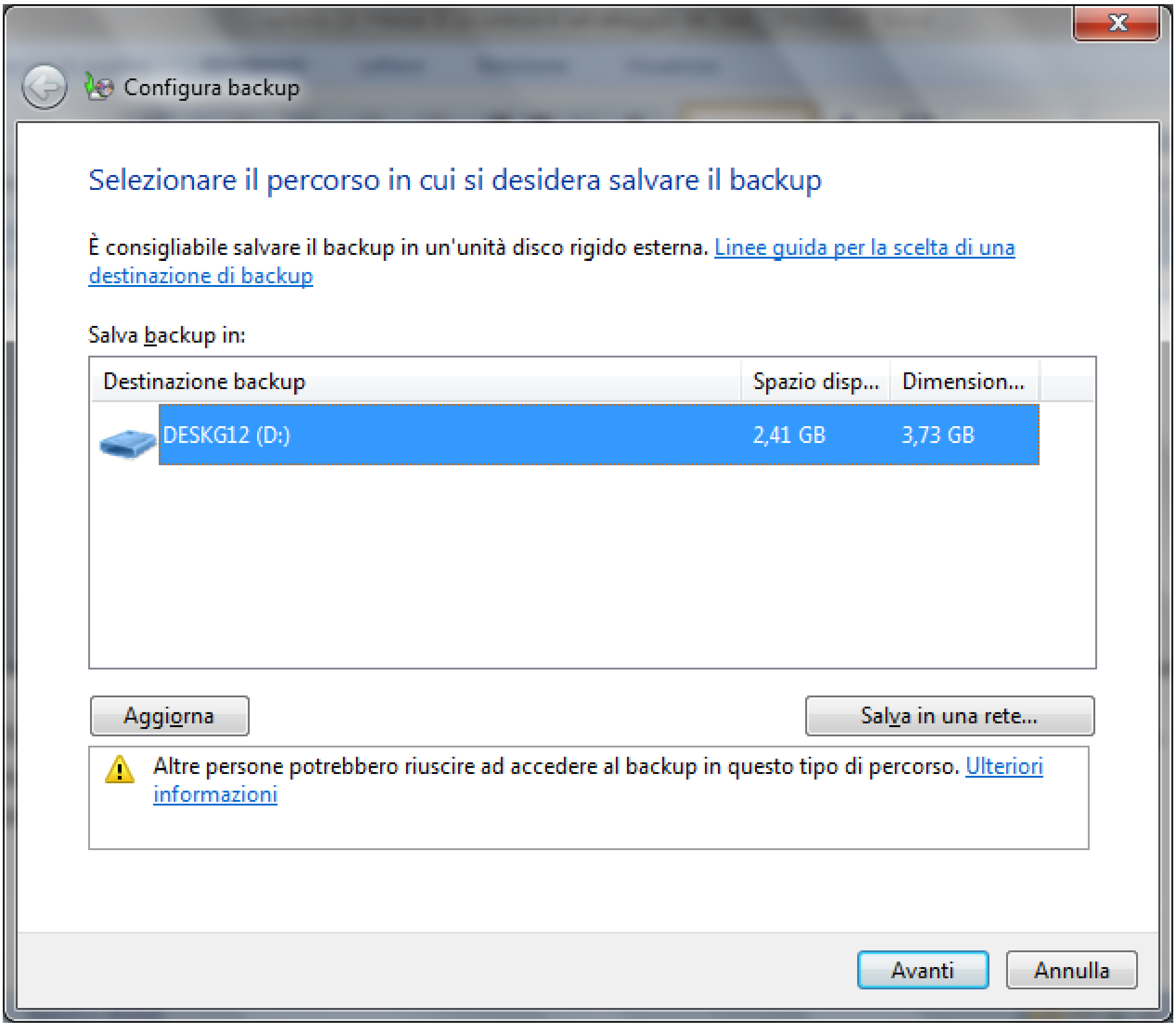
Con **Backup e ripristino**, presente nel Pannello di controllo di Windows 7, si possono creare copie di sicurezza dei file più importanti, in modo da poter affrontare qualsiasi emergenza.



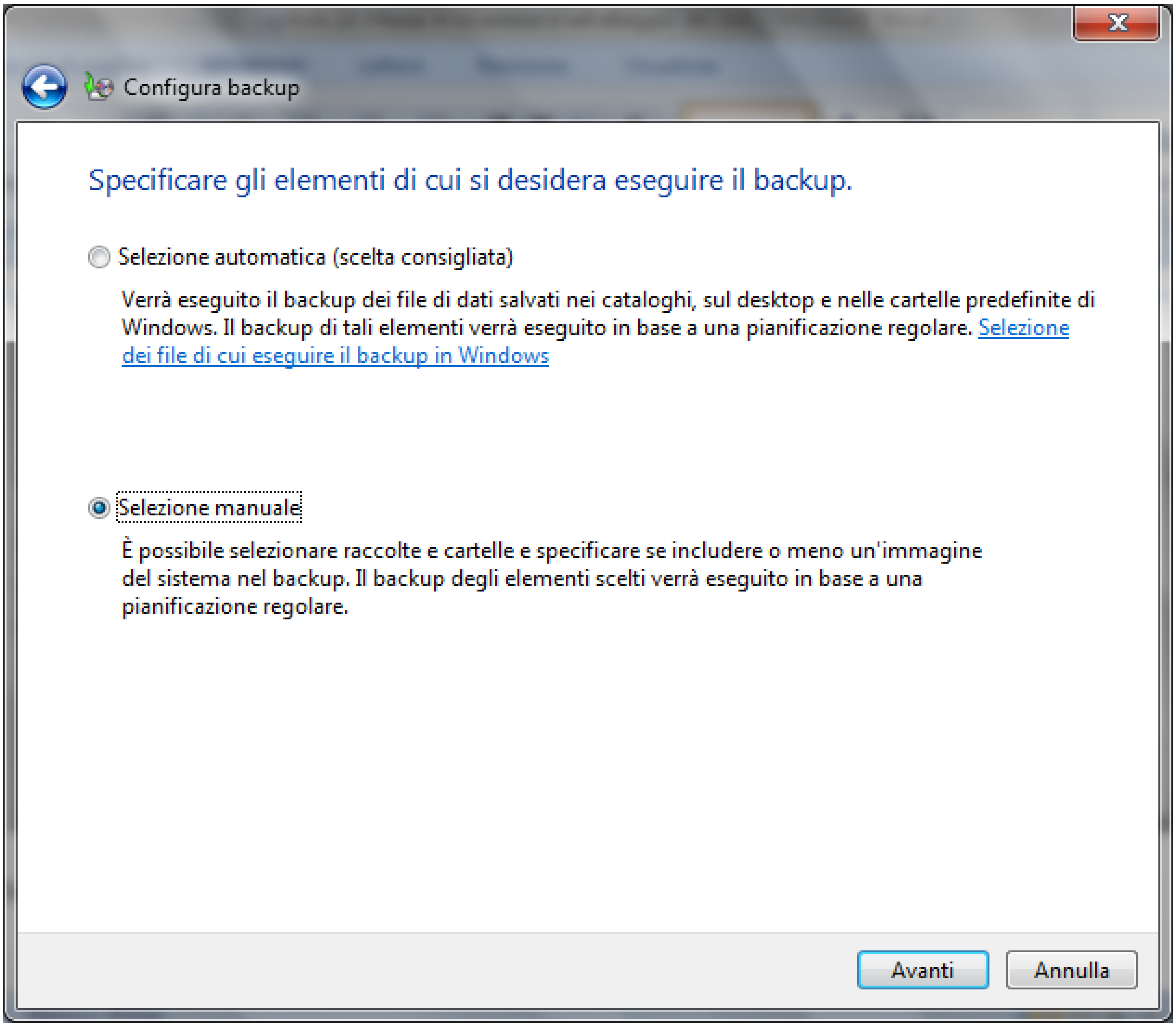
Se non si è mai utilizzato Windows Backup, fare clic su **Configura backup** per avviare la relativa procedura guidata.



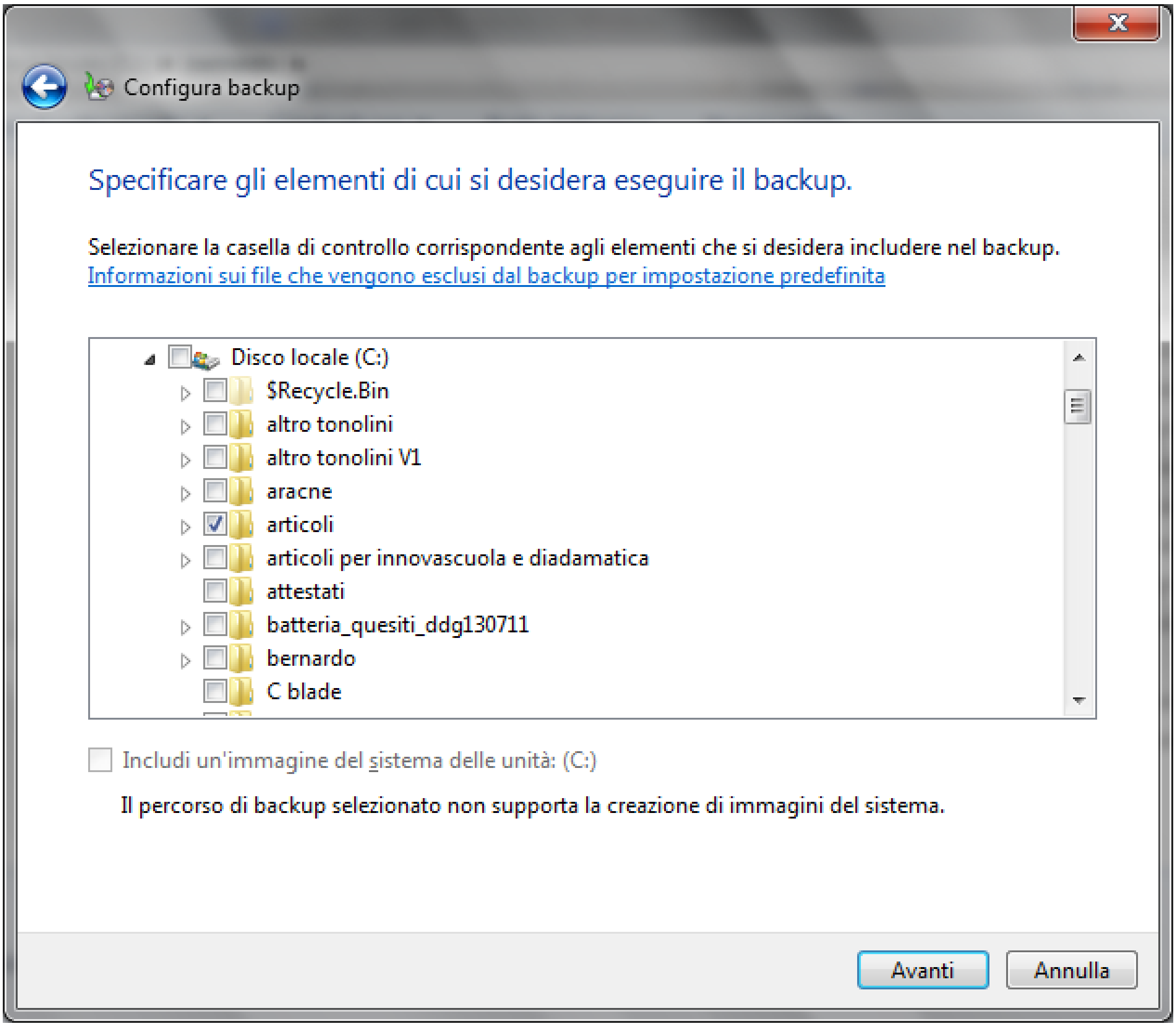
Nel primo passaggio si deve indicare il supporto dove memorizzare il backup. È consigliabile non eseguire il backup dei file sullo stesso disco rigido in cui è installato Windows. Nel nostro caso utilizziamo un chiavetta USB.



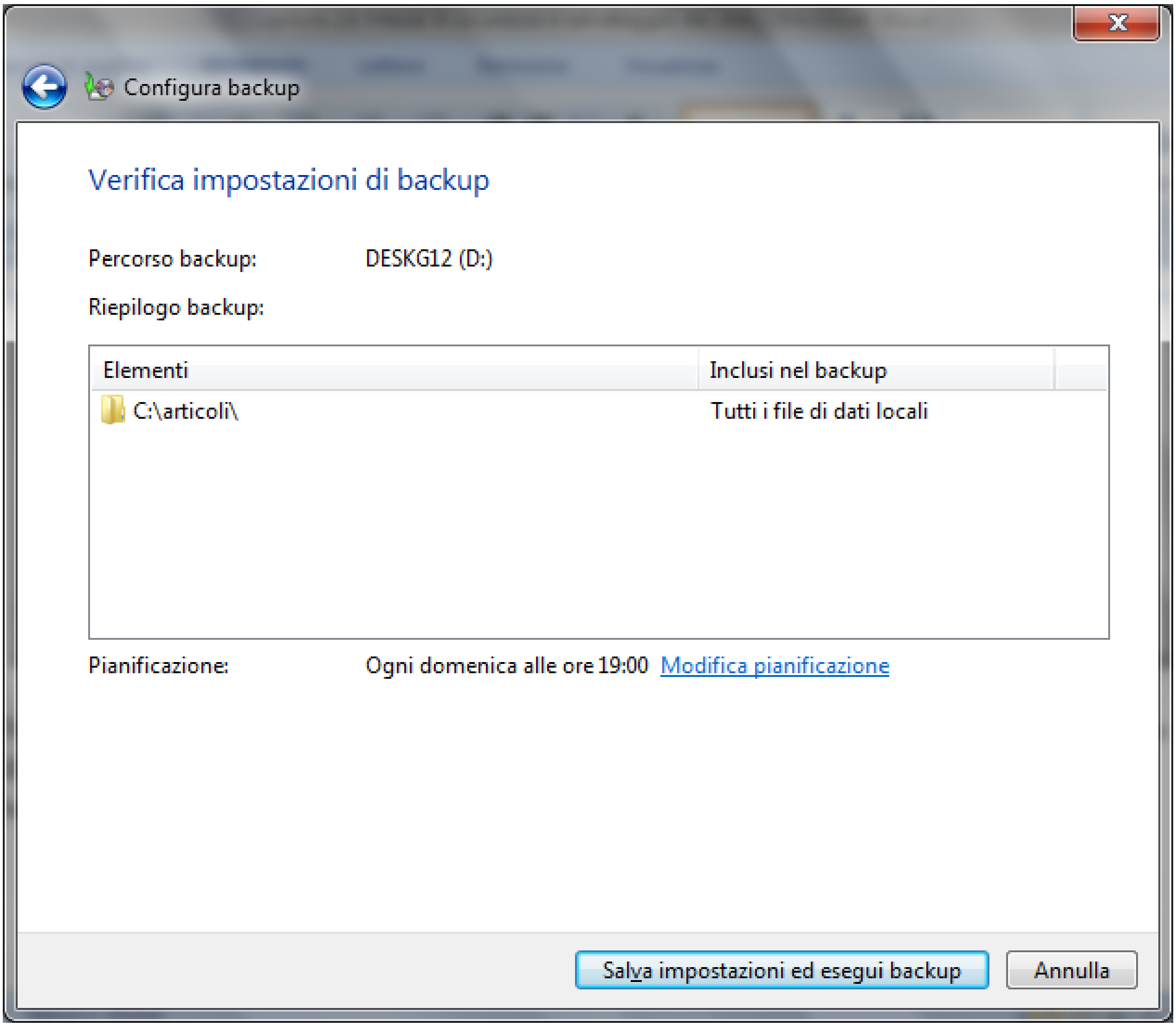
Il secondo passaggio, è relativo a come scegliere i file oggetto del backup.



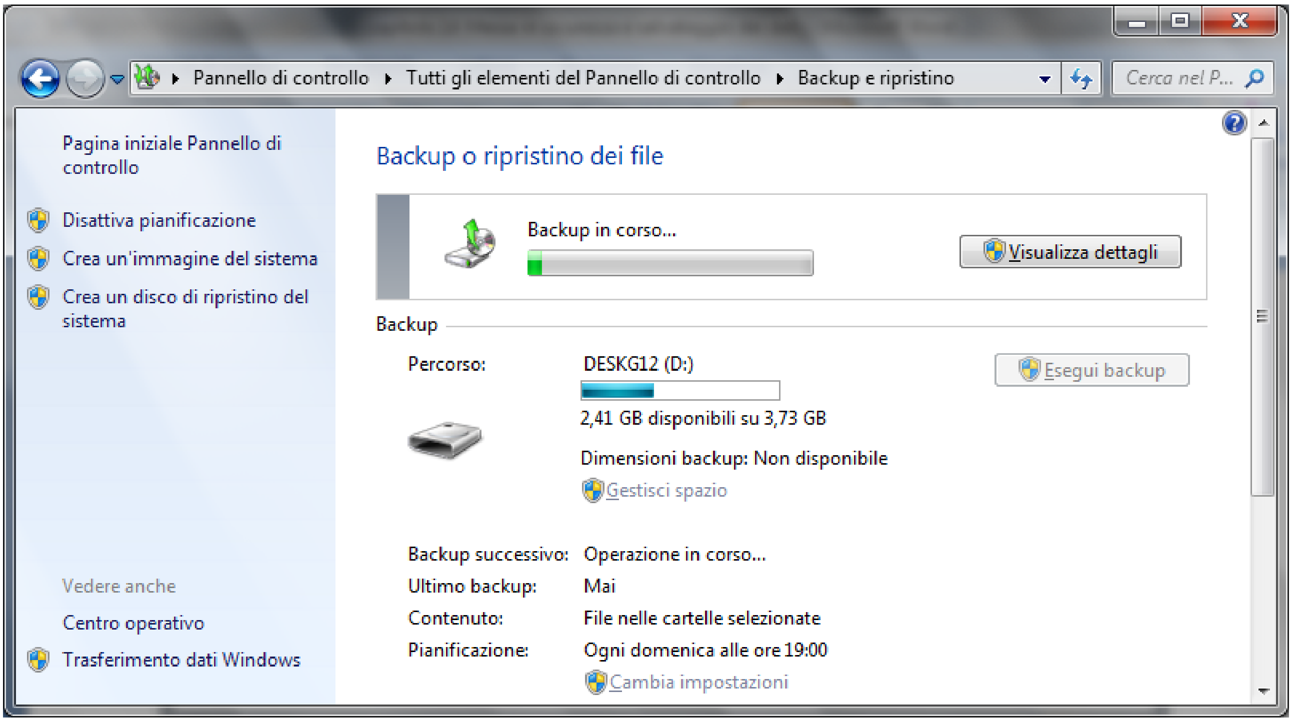
È possibile lasciare che sia Windows a scegliere gli elementi da sottoporre a backup oppure è possibile selezionare singolarmente le cartelle e le unità desiderate.
Nel caso di **Selezione automatica**, nel backup saranno inclusi i file salvati nelle raccolte (Immagini, Documenti, Musica, Video), sul desktop e nelle cartelle predefinite di Windows.
Nel nostro caso proviamo la **Selezione manuale**, per scegliere dei file specifici.



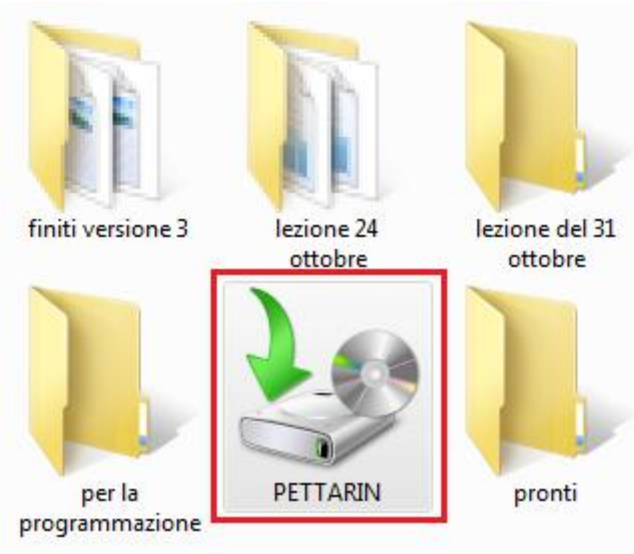
La finestra permette di selezionare le cartelle da includere nel backup, evidenziate con un segno di spunta nella rispettiva casella. Con un clic su **Avanti** si visualizza il riepilogo del processo di backup creato.



Con il pulsante **Salva impostazioni e esegui backup** si avvia il processo di copia.

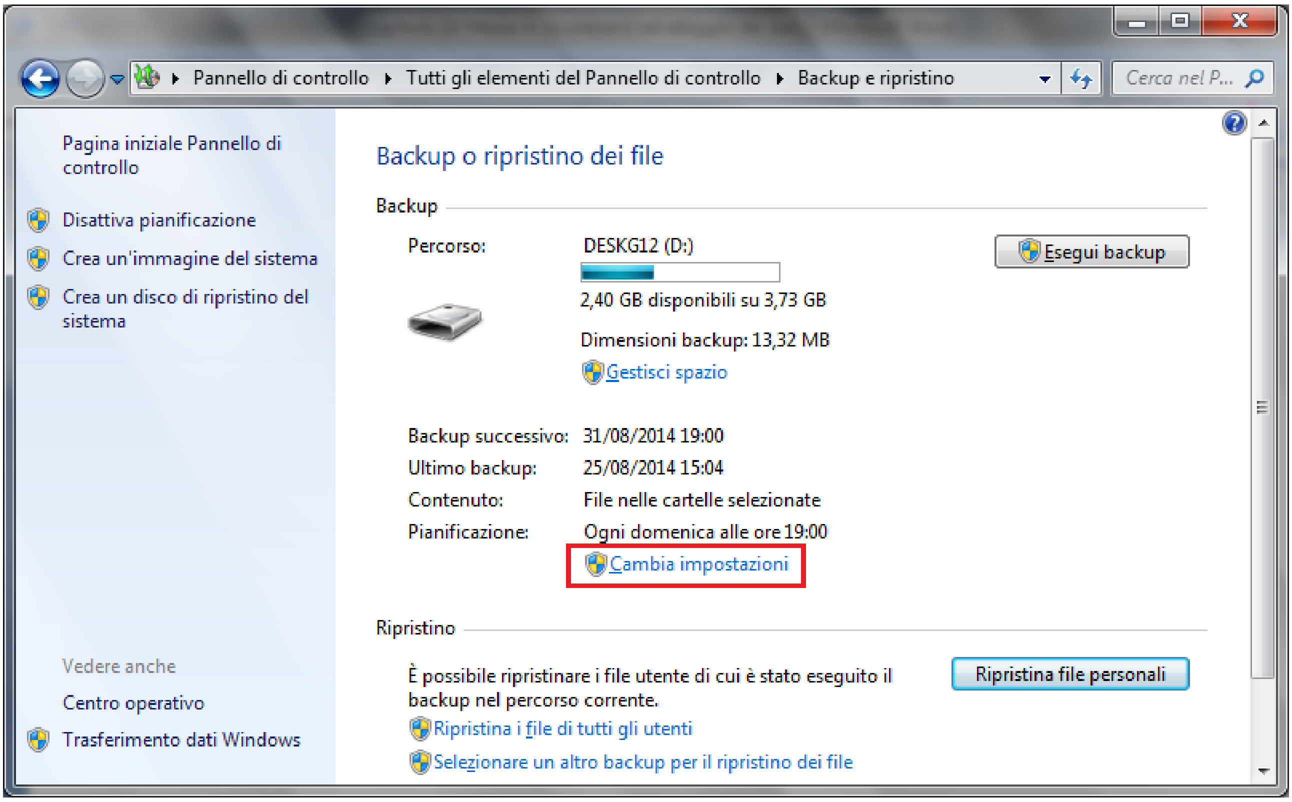


La procedura guidata di backup è terminata. Nel supporto di memoria è presente la copia di sicurezza.

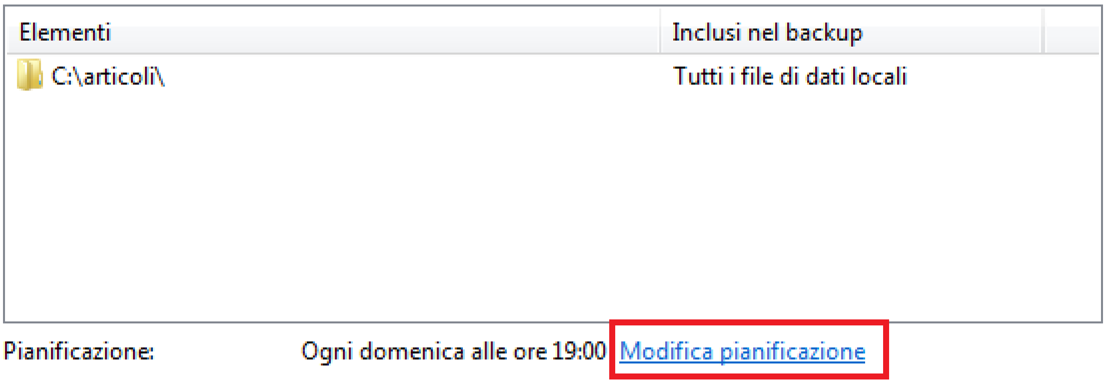


Pianificare il backup

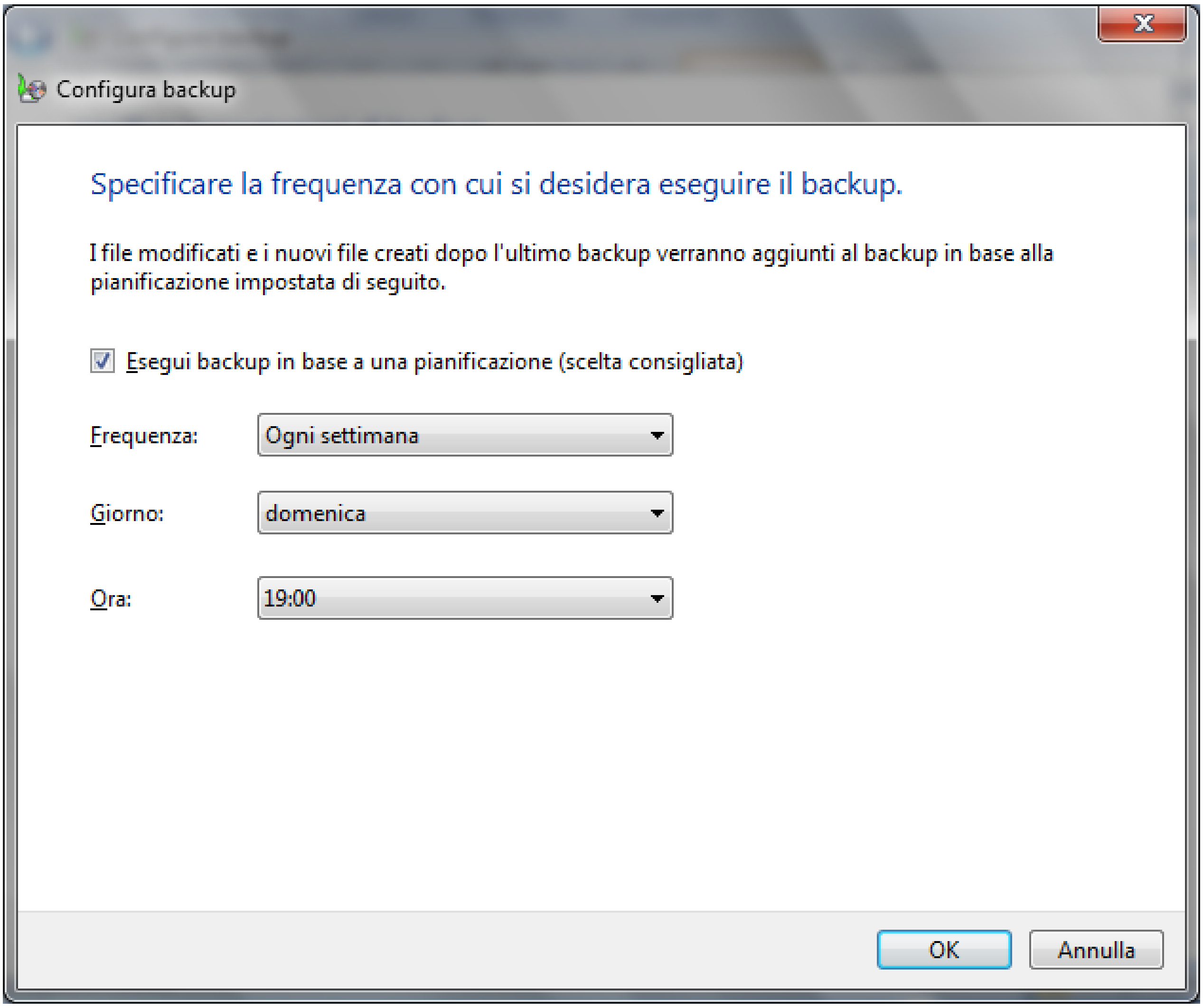
La procedura guidata crea automaticamente una pianificazione del backup. Con questa pianificazione, non è più necessario ricordarsi di fare il backup dei file.
Le impostazioni di backup automatico, ad esempio la frequenza del backup, il tipo di archiviazione da utilizzare o i tipi di file da sottoporre a backup, possono essere modificate in qualsiasi momento, con un clic sul comando **Cambia impostazioni**.



Sono riproposti i passaggi della procedura guidata del backup. Al quarto passaggio, fare clic su **Modifica pianificazione**.

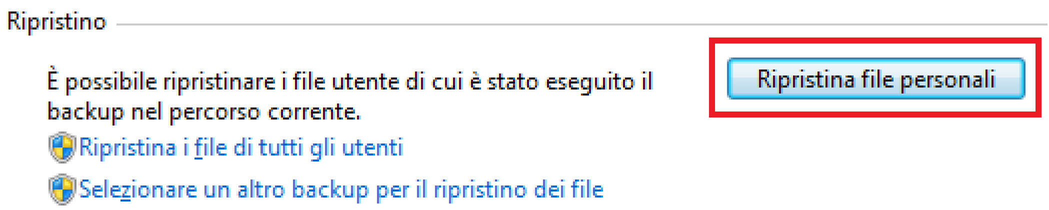


La finestra permette di modificare la pianificazione con gli appositi menu a discesa.

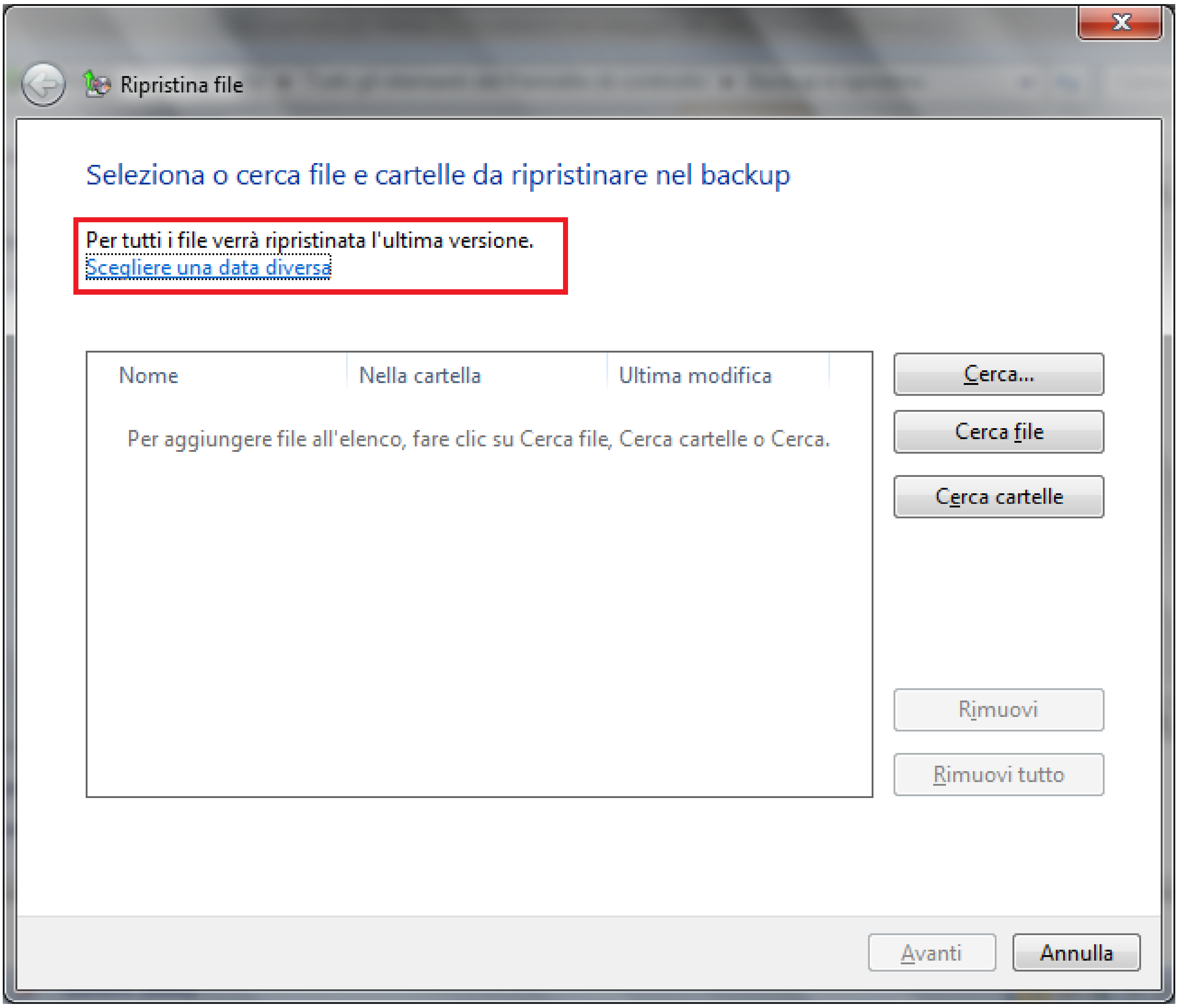


Ripristinare i dati

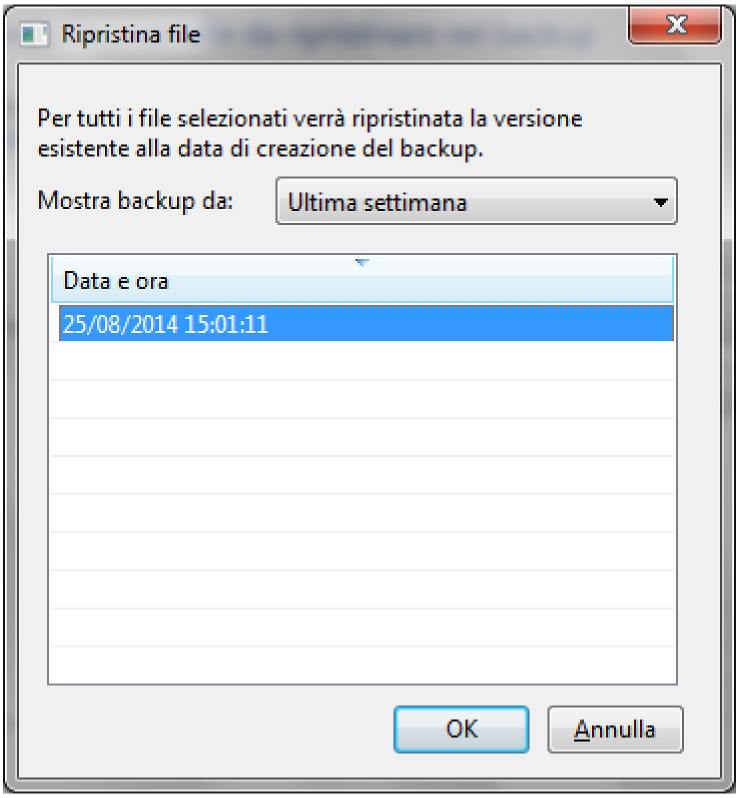
La procedura inversa del backup è il *ripristino* dei dati salvati. Se non si riesce a trovare un file nel computer, si è accidentalmente modificato o eliminato un file, o semplicemente si vuole riavere una copia precedente, è possibile ripristinarlo dal backup con un clic su **Ripristina file personali**.



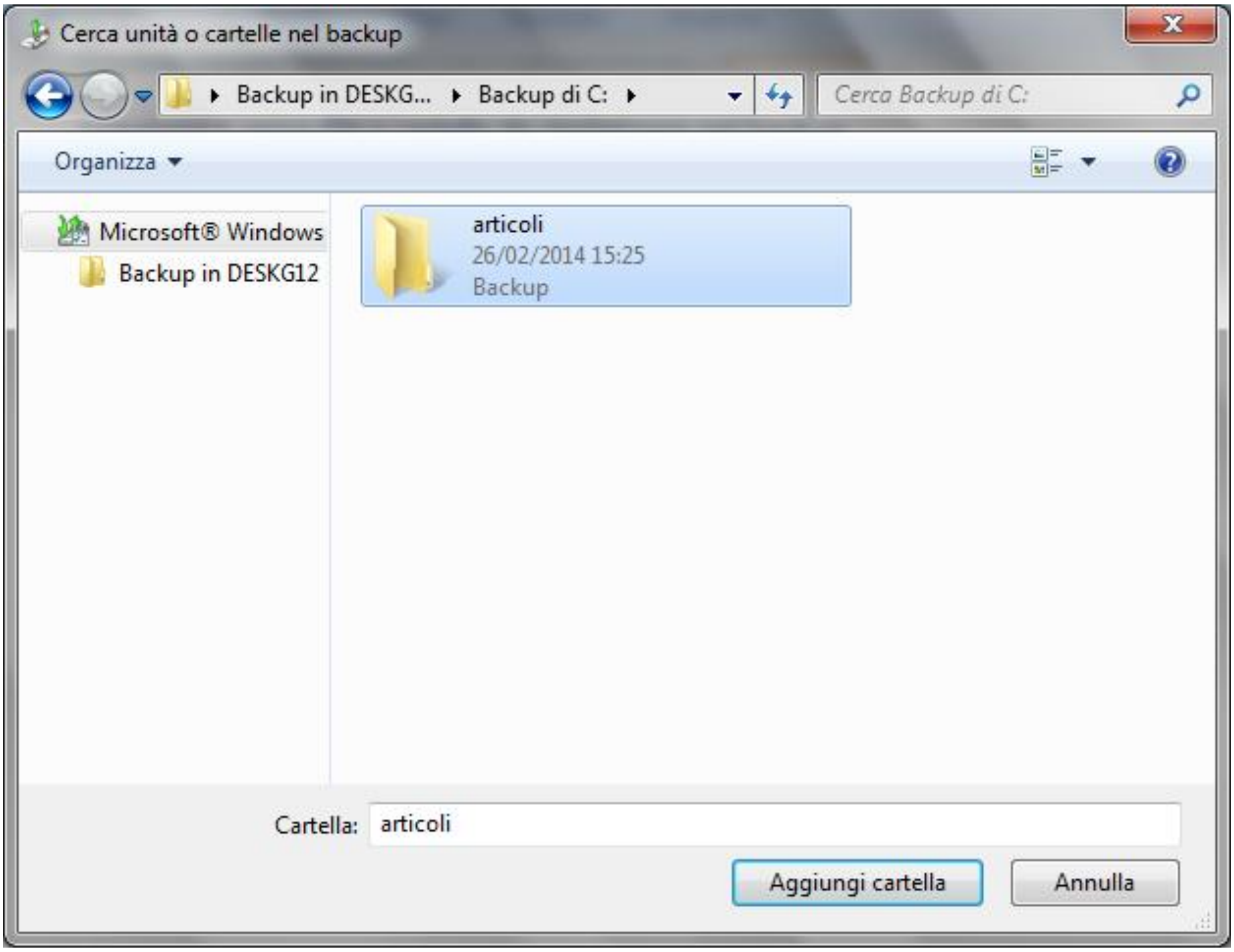
Anche in questo caso è proposta una procedura Guidata. Con la prima finestra si sceglie se ripristinare l'ultima versione o versioni di backup precedenti. Questa particolarità è chiamata **Versioning**.



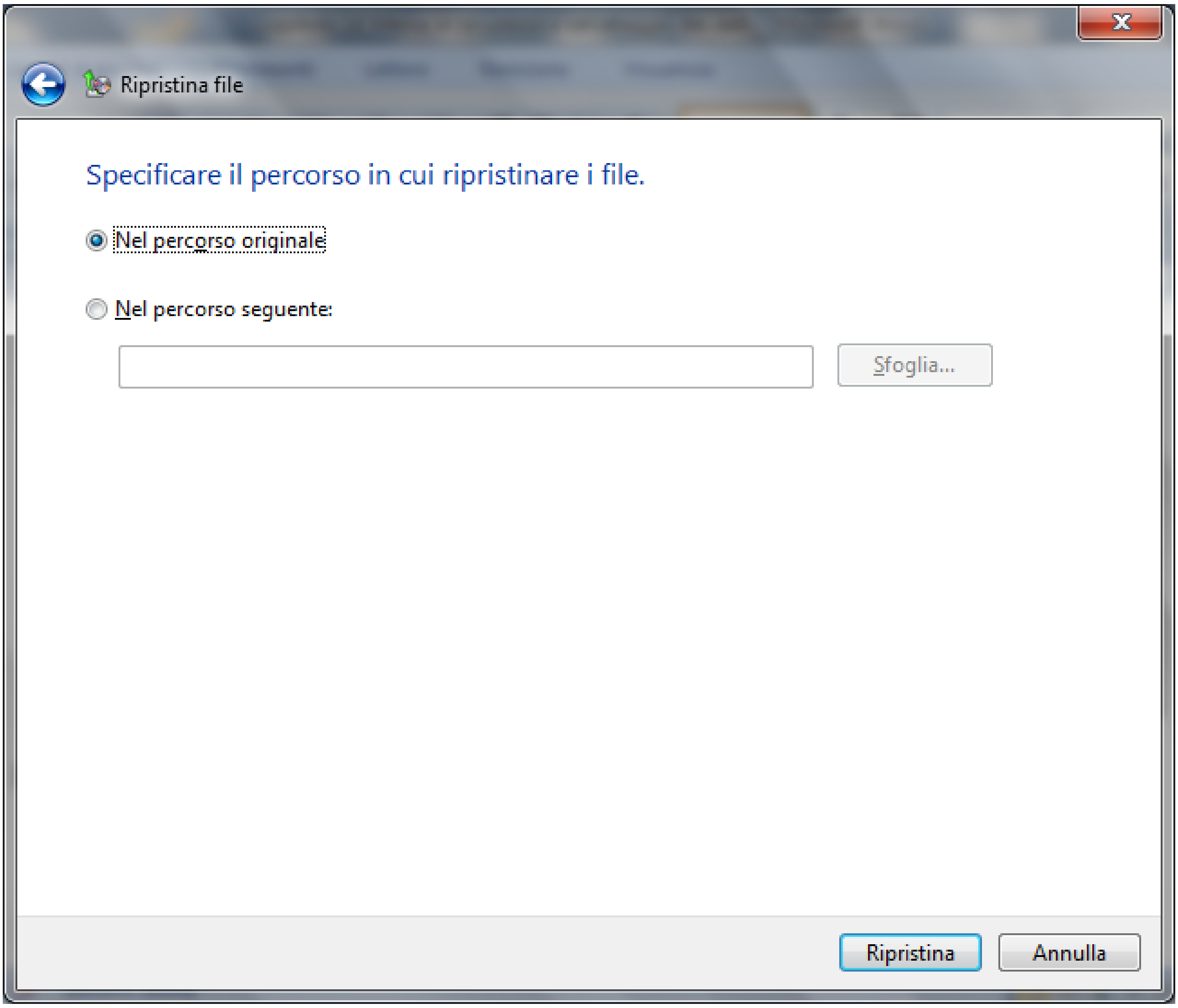
Le varie versioni si selezionano con un clic su **Scegliere una data diversa**.



Una volta scelta la versione, con i pulsanti **Cerca cartelle** e/o **Cerca file** (Per visualizzare i singoli file. Quando si ricercano cartelle, non si può visualizzare i singoli file in esse contenuti) è possibile selezionare cosa ripristinare.



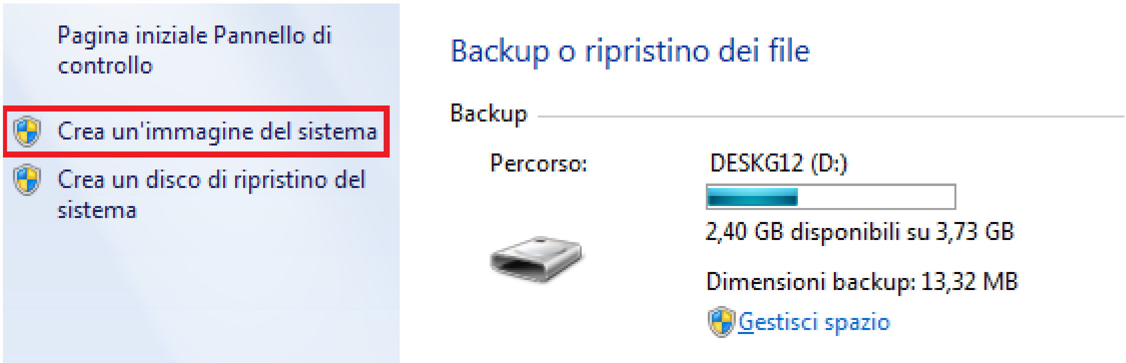
Le cartelle (e i file) da ripristinare si inseriscono con **Aggiungi cartella**. Proseguire con **Avanti**.



La procedura è quasi conclusa. Basta specificare se i file ripristinati vanno inseriti nella posizione originaria o si vuole cambiare percorso di memorizzazione. Premere **Ripristina** per concludere la procedura.

Creare un’immagine del sistema

È possibile creare un'immagine del sistema che includa una copia di Windows e copie dei programmi, delle impostazioni di sistema e dei file, con un clic su **Crea un’immagine del sistema**.



L'immagine del sistema una volta archiviata in una posizione separata si può utilizzare per ripristinare il contenuto del computer se il disco rigido o l'intero computer smette di funzionare.

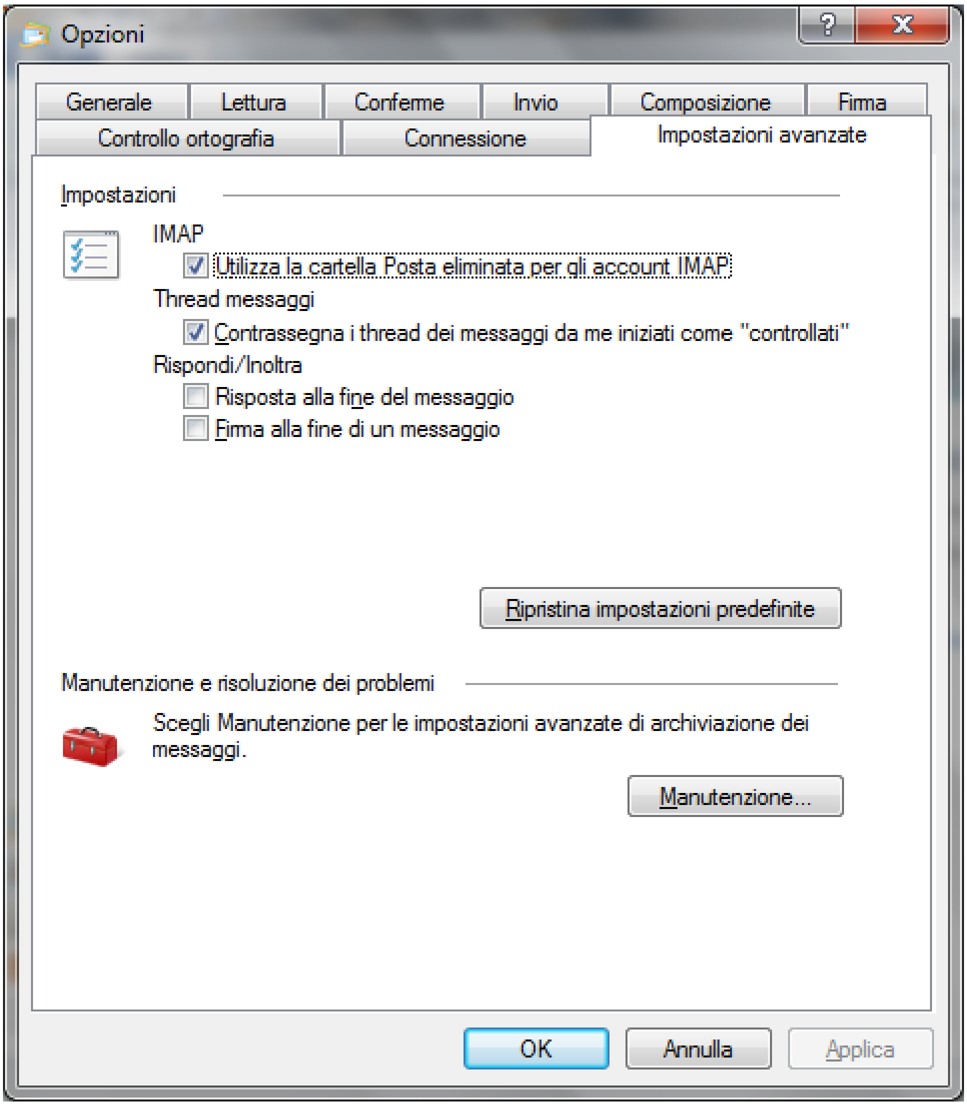
Backup dei Preferiti, Mail, Rubrica e Cronologia

Vediamo dove Windows 7 memorizza alcuni file particolari.

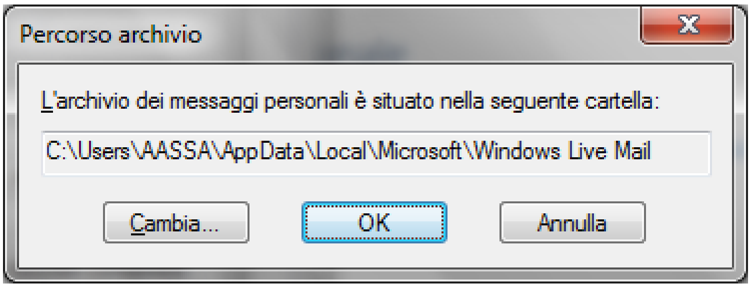
Siti preferiti di Internet Explorer: si trovano in C:\Utenti\NomeUtente\Preferiti.

Cronologia e altri file temporanei di Internet Explorer: si trovano in C:\Users\NomeUtente\AppData\Local\Microsoft\Windows\Temporary Internet Files

Mail di Windows Live Mail: per vedere in quale cartella sono memorizzate le mail inviate e ricevute si apra le **Opzioni** delle **Mail**.



Nella scheda **Impostazioni avanzate** fare clic su **Manutenzione**. Appare il percorso di memorizzazione dei messaggi personali.



In generale il percorso è: C:\Utenti\NomeUtente\Local\Microsoft\Windows Live Mail. Nella stessa cartella è presente la **Rubrica**.

Domande

1. Per un backup efficiente è importante
    a. dove conservare le copie
    b. frequenza delle copie
    c. Quali dispositivi utilizzare.
    d. Tutte le affermazioni sono corrette
2. Dove è meglio conservare un backup?
    a. su un disco rigido interno
    b. su un disco rigido esterno ma costantemente collegato al computer
    c. su un disco rigido esterno collocato in un luogo diverso da dove sono i dati originali
    d. sullo stesso disco rigido dove sono i dati originali
3. Una copia di sicurezza creata con Windows Backup viene controllata, quindi è sicura dalla presenza di malware
    a. È sicura solo per i Trojan
    b. È sicura solo per i Worm
    c. È sicura solo per i virus da Macro
    d. Falso
4. Cosa significa "Versioning" nell'ambito del backup informatico?
    a. Varie traduzioni di un documento (serve a vedere anche i salvataggi precedenti)
    b. Partizione dell'Hard Disk
    c. Tipo di backup
    d. Tutte le risposte sono errate
5. Quale supporto di memoria è più adatto per il backup dei dati?
    a. Hard Disk esterno
    b. CD ROM
    c. Hard disk interno
    d. Floppy disk

Capitolo 15

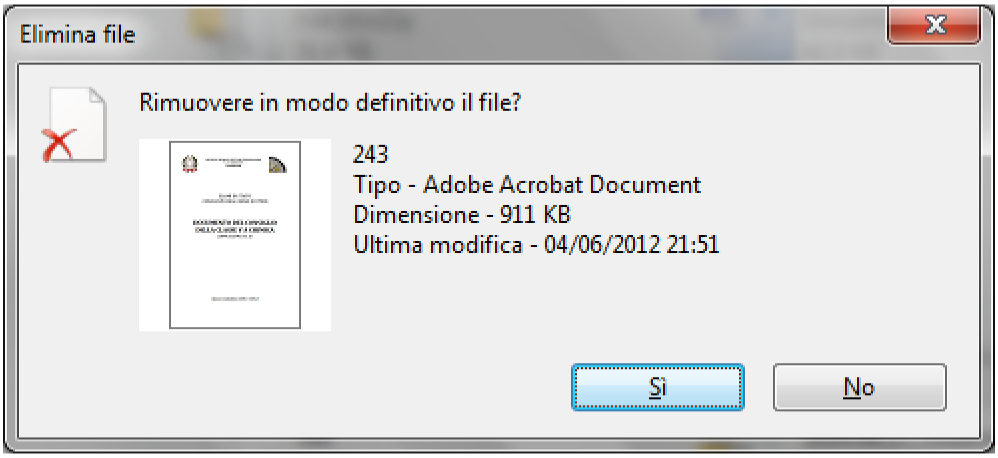
Distruzione sicura dei dati

Importanza di una eliminazione definitiva dei dati

Quando non sono più essenziali, è necessario che i dati sensibili di qualsiasi tipo, commerciale, finanziario o dati personali, siano cancellati in modo assolutamente sicuro, in modo che non possano essere recuperati da terzi.

Differenza tra cancellare i dati e distruggerli in modo permanente

La cancellazione dei file non equivale alla rimozione effettiva di essi dal computer.
Quando si cancella un file non "sparisce" dall'hard disk, ma viene posto in una parte della memoria, il Cestino, da dove è possibile recuperarlo. È poi possibile cancellare il file anche dal Cestino.
Se si cancella un file da un dispositivo di memoria diverso dall'hard disk non c'è il passaggio dal Cestino. La cancellazione è immediata.
Il messaggio di Windows, che appare quando si elimina dal Cestino, è il seguente.



A questo punto il file non è più visibile, quindi non si può recuperare con il comando Ripristina.
In realtà il file è ancora presente nell'Hard disk (o nel dispositivo esterno) anche se la sua icona non è più visibile. Infatti, il sistema operativo Windows non cancella subito dalla memoria i file eliminati, ma "segna" lo spazio di memoria che essi stanno occupando come disponibile per la memorizzazione (futura) di altri file. Questo spazio verrà occupato solo quando un file, da inserire in memoria, non troverà altro spazio libero di memoria: il file cancellato sarà allora (definitivamente) rimosso, e il suo posto viene occupato dall'altro file.
Chiaramente, con le dimensioni degli hard disk attuali, un file cancellato può tranquillamente restare presente in memoria per anni e anni.

Questo concetto è importante, dato che ci sono dei programmi (disponibili dai rivenditori di computer o in Internet) che permettono di recuperare anche i file cancellati dal Cestino, in modo definitivo.

Metodi software per distruggere i dati in modo permanente

Abbiamo visto che le normali operazioni di cancellazione dei file sono insufficienti a garantire la reale eliminazione dei dati in questione. Con semplici software è ormai possibile recuperare i file eliminati dal Cestino (anche dopo averlo svuotato).
Come è possibile distruggere i dati in modo permanente nel momento che non servono più e non si vuole che finiscano in mano a soggetti terzi?
Sbarazzarsi dei vecchi pc potrebbe essere un'operazione pericolosissima: i magazzini abbandonati e le discariche di materiale elettronico sono i luoghi preferiti dai cracker per effettuare trashing.
Pertanto, è di vitale importanza che chi gestisce tali postazioni, sia esso una istituzione finanziaria, un ente pubblico o un ufficio privato, dedichi la giusta attenzione al problema della cancellazione sicura dei dati, eliminando in maniera definitiva ed irreversibile le informazioni precedentemente salvate, evitando qualsiasi possibile problema, anche involontario, di violazione della privacy o di accesso a dati riservati.
Senza una adeguata protezione, informazioni riservate, dati di accesso, numeri di carte di credito o contratti privati potrebbero essere (volontariamente o meno) diffusi all’esterno, rischiando di cadere nelle mani sbagliate, con tutti i rischi di tali situazioni.
Nel caso di documenti cartacei la soluzione migliore è l’utilizzo di tritadocumenti, che tagliano a striscioline o riducono a coriandoli i fogli.



Nel caso di informazioni in formato non cartaceo la situazione è più complessa.
Teoricamente la cancellazione definitiva avviene solamente con la formattazione dell’unità di memoria. Ma una formattazione “morbida”, come la formattazione veloce, rimuove solo la tabella di allocazione e non intacca i dati.
Più lungo e affidabile è invece il sistema con cui i blocchi vengono interamente rimpiazzati da dati casuali. La cancellazione via software ha però un punto debole, insito nella natura magnetica del supporto. La riscrittura sistematica di dati sulla superficie del disco non garantisce la distruzione delle informazioni presenti in passato, che permangono sotto forma di flebili tracce sulle piattine, tracce rilevabili e interpretabili.
L’operazione non è alla portata di chiunque: richiede camere sterili e strumenti specifici come i microscopi che rilevano le forze magnetiche. È utilizzata in ambito poliziesco. Sono in grado di recuperare, tra gli altri, i dati contenuti in dischi bagnati in acqua o altri liquidi o colpiti da fulmini e scariche elettriche.

Metodi hardware per distruggere i dati in modo permanente

In alternativa è possibile agire con la forza bruta, ad esempio smagnetizzando il supporto elettronico, tramite l'esposizione ad un forte campo magnetico che finisce per eliminare tutte le informazioni ed i dati salvati al suo interno.
Un approccio "fisico" è più esigente e pesante ma anche più definitivo e soddisfacente anche se a fronte di un po' di lavoro e l'impiego di attrezzi pesanti. Esistono direttive di governi, enti sanitari e aziende che impongono questo tipo di distruzione cruenta dei dischi.
Tra i metodi più usati abbiamo la distruzione a colpi di martello e piccone, la trapanazione, il degaussing o l'inceneritura, tutte modalità che compromettono in maniera permanente la superficie su cui sono scritti i dati.
Non dimentichiamo nemmeno dei supporti ottici: CD e DVD non hanno la vulnerabilità analoga ai supporti magnetici ma rappresentano anche loro un problema da risolvere. La scelta è vasta e include l'incidere o graffiare la superficie del CD o di spezzarlo.

Cosa dice la legge

Dal punto di vista legale, la legislazione sulla privacy prevede e regolamenta la cancellazione sicura dei dati contenuti su supporti elettronici, che prima di essere usati di nuovo o eliminati, devono essere trattati con sistemi che garantiscano che i dati in essi precedentemente contenuti non possano essere recuperati o ricostruiti, e che sia impossibile leggerli.
La non osservanza di tale disposto legislativo potrebbe portare a sanzioni amministrative o addirittura penali.

Domande

1. È necessario che i dati sensibili siano cancellati in modo assolutamente sicuro?
    a. Solo quelli di tipo commerciale
    b. Solo quelli di tipo finanziario
    c. Solo i dati personali
    d. Tutti i dati sensibili
2. La cancellazione dei file non equivale alla rimozione effettiva di essi dal computer
    a. È vero
    b. È falso
    c. È vero solo se si cancella dall'hard disk
    d. È vero solo se si cancella dalle chiavi USB
3. In generale è possibile recuperare anche i file cancellati dal Cestino
    a. No, mai
    b. Dipende dalla dimensione del file
    c. In genere sì, con degli appositi programmi
    d. Dipende dal tipo di file
4. La formattazione veloce
    a. Rimuove tutti i file
    b. Rimuove solo la tabella di allocazione e non intacca i dati
    c. Rimuove i dati ma non la tabella di allocazione
    d. Tutte le affermazioni sono errate
5. Quali sono dei metodi di distruzione fisica dei supporti di memorizzazione?
    a. Distruzione a colpi di martello e piccone
    b. La trapanazione
    c. L'inceneritura
    d. Tutte le risposte sono corrette

Soluzioni di tutte le domande

CAP 1: A, D
CAP 2: D, D, B
CAP 3: A, A, D, B
CAP 4: B, D, D
CAP 5: C, B, A, B, D, D
CAP 6: D, A, C, A, D, A
CAP 7: D, A, D, D, D, A, B, B, A
CAP 8: C, B, A, B, B, C, A, C, C, D
CAP 9: D, D, A
CAP 10: A, B, C, B, D, C, B, B
CAP 11: C, C, A, A, B, D, B
CAP 12: D, D, A, D, A, D, B
CAP 13: C, A, D, D, D
CAP 14: D, C, D, A, A
CAP 15: D, A, C, B, D